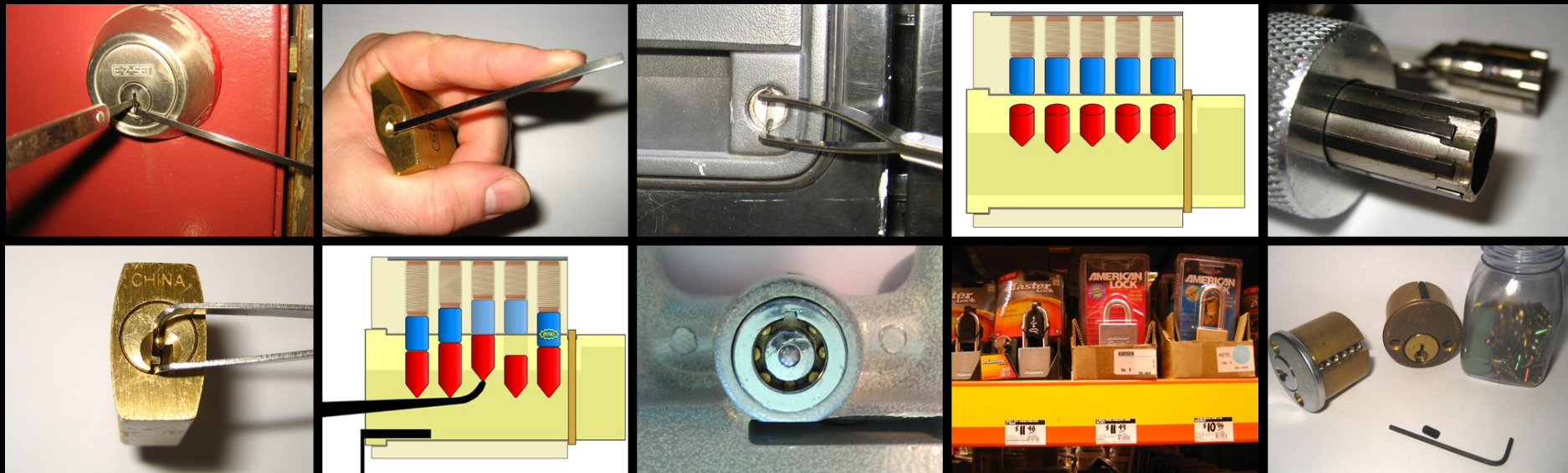


New

Ten Things You Should Know About Lockpicking

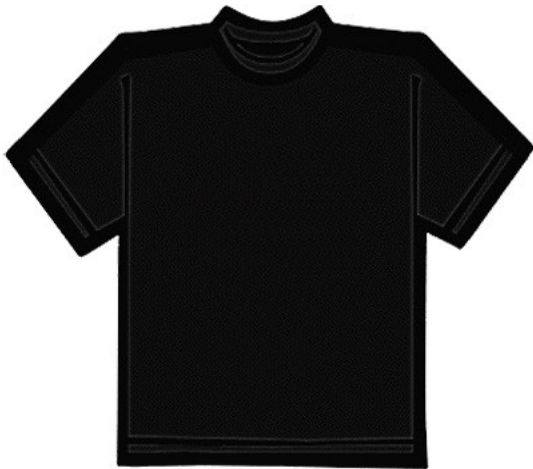


by Deviant Ollam
Event Name
XXXX-XX-XX

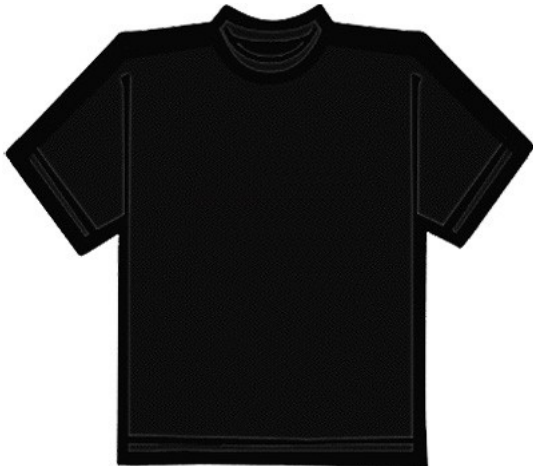
Who am i ?



Who am i ?



Who am i ?



**THE
CORE
GROUP**

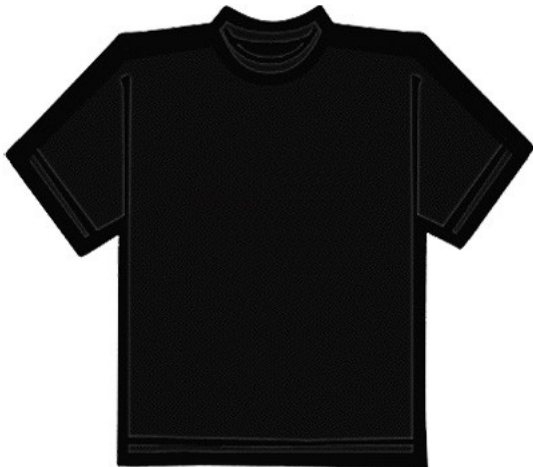
**auditing
assessments
research
trainings**

Who am i ?



**THE
CORE
GROUP**

**auditing
assessments
research
trainings**



**workshops
public lectures
lockpick village
contests & games**

Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals









All your hard work here...



All your hard work here...gets
unlocked here



Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal

Pin Tumbler Locks



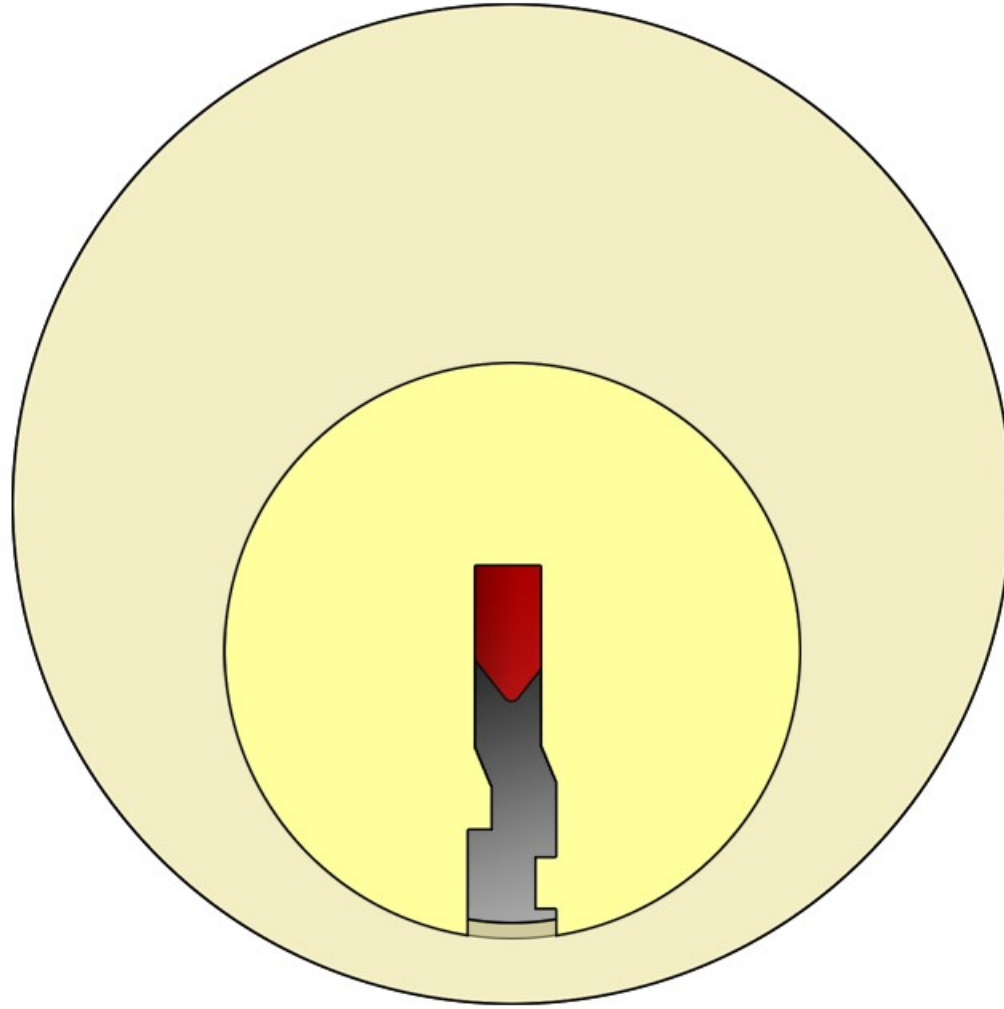
Pin Tumbler Locks



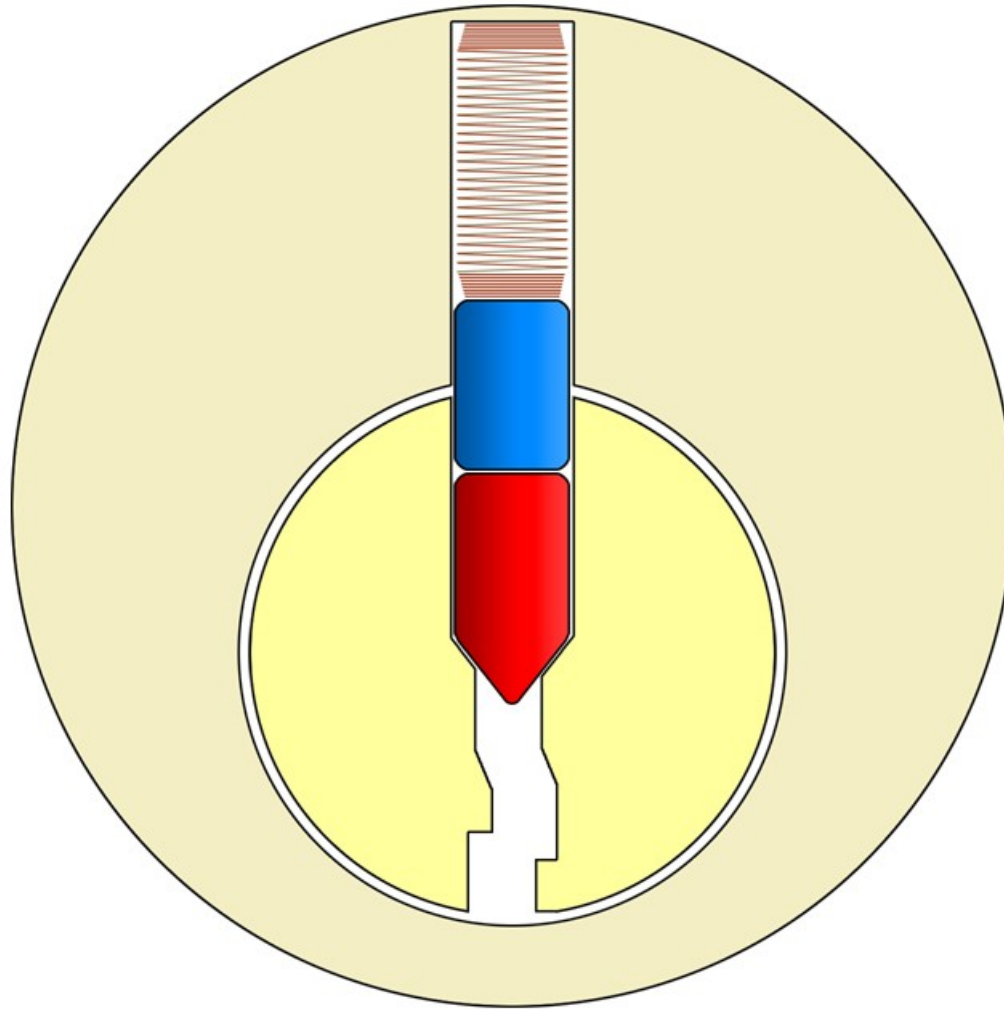
Pin Tumbler Locks



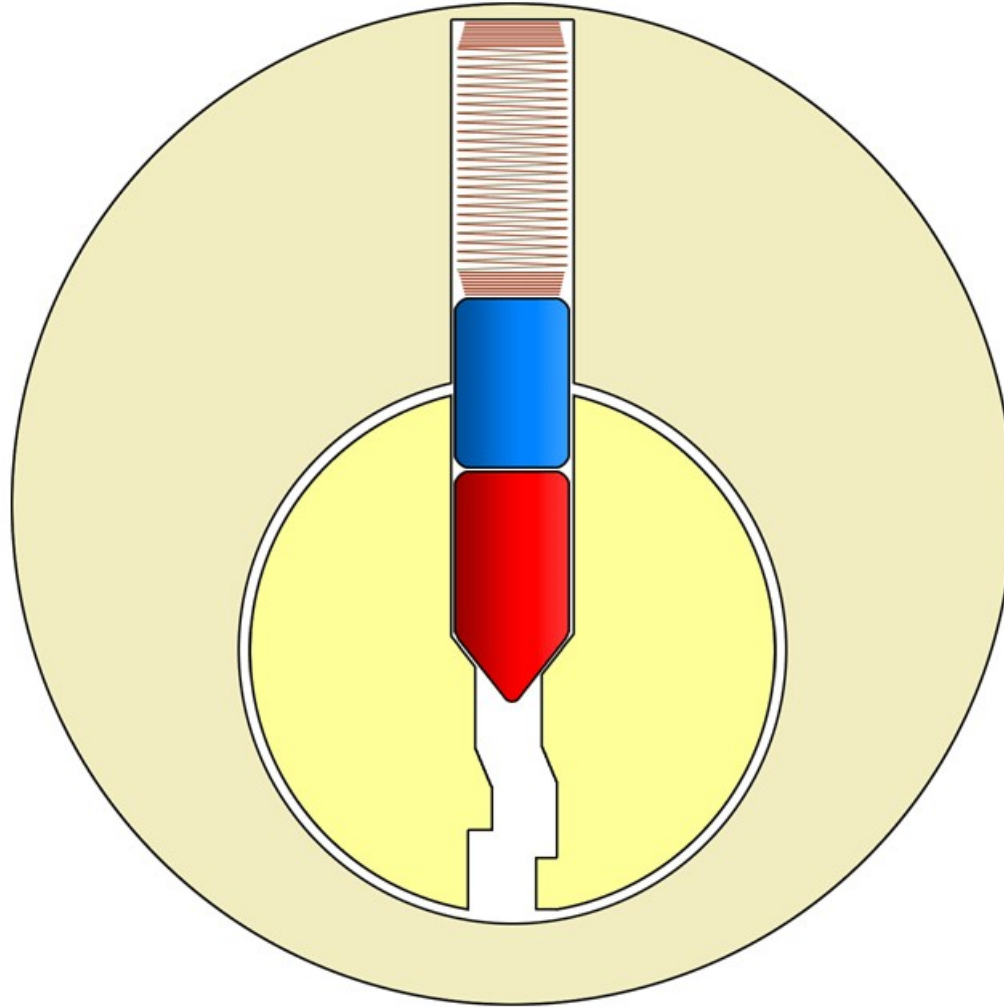
The View From Outside



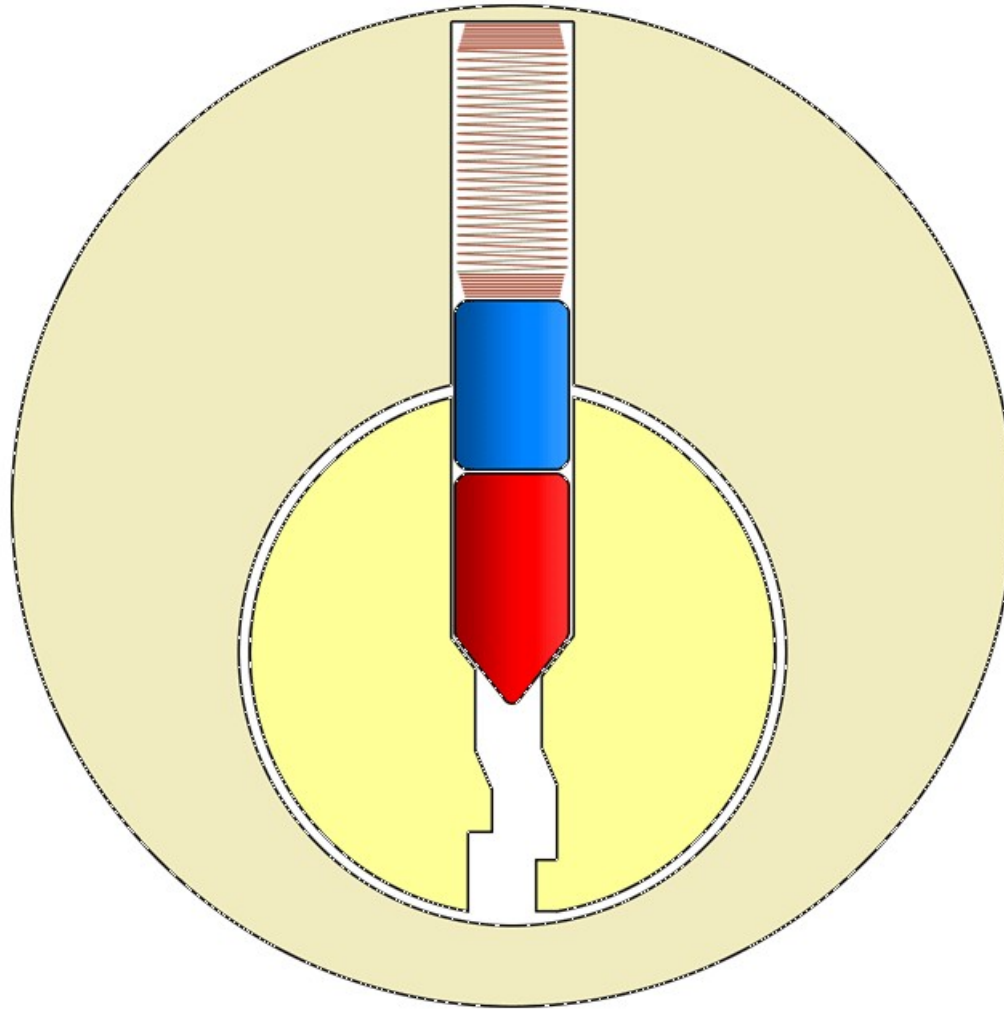
What's On The Inside



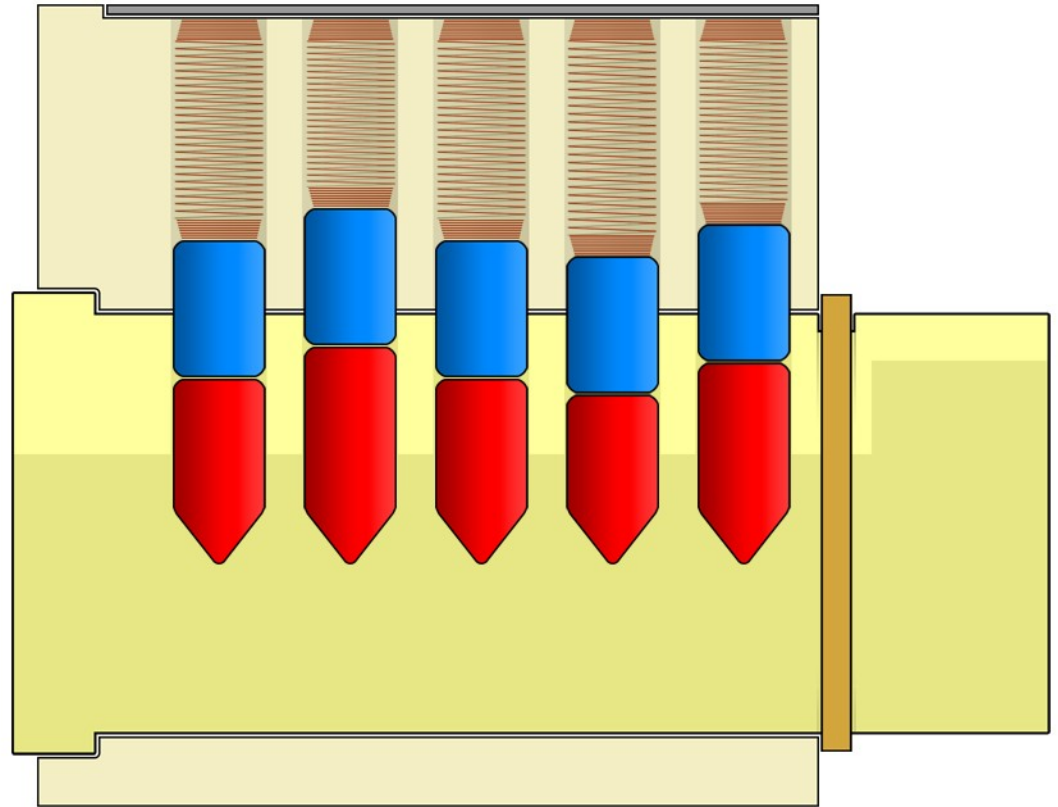
What's On The Inside



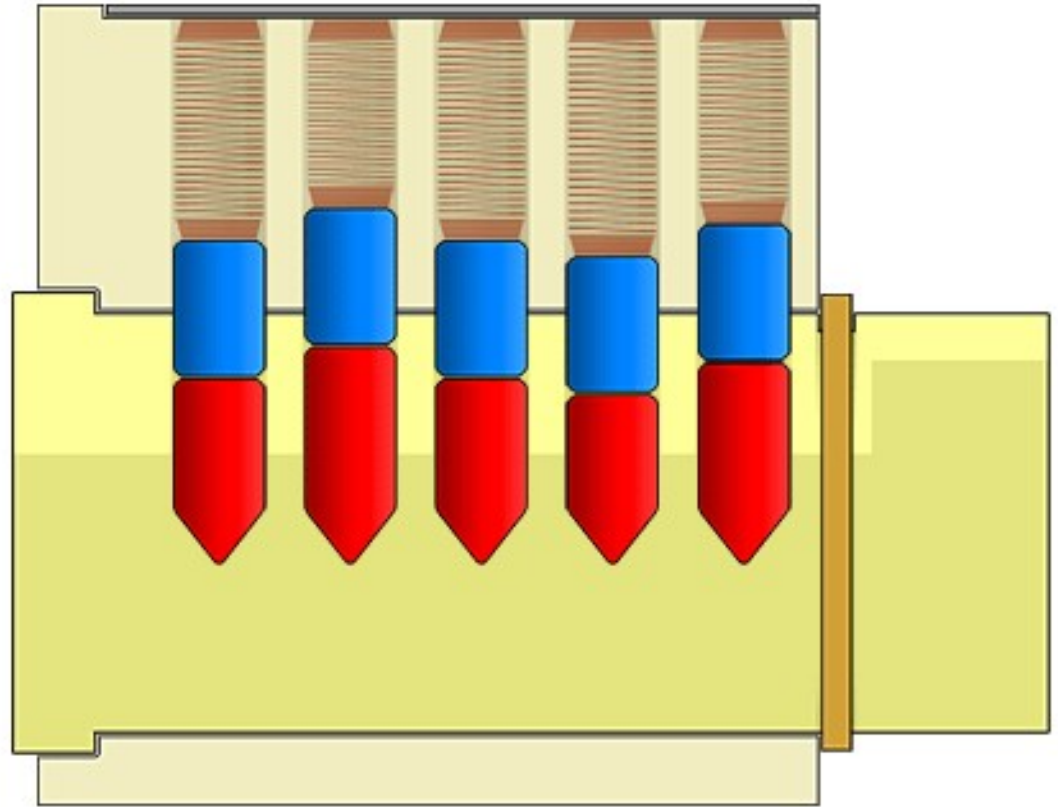
What's On The Inside



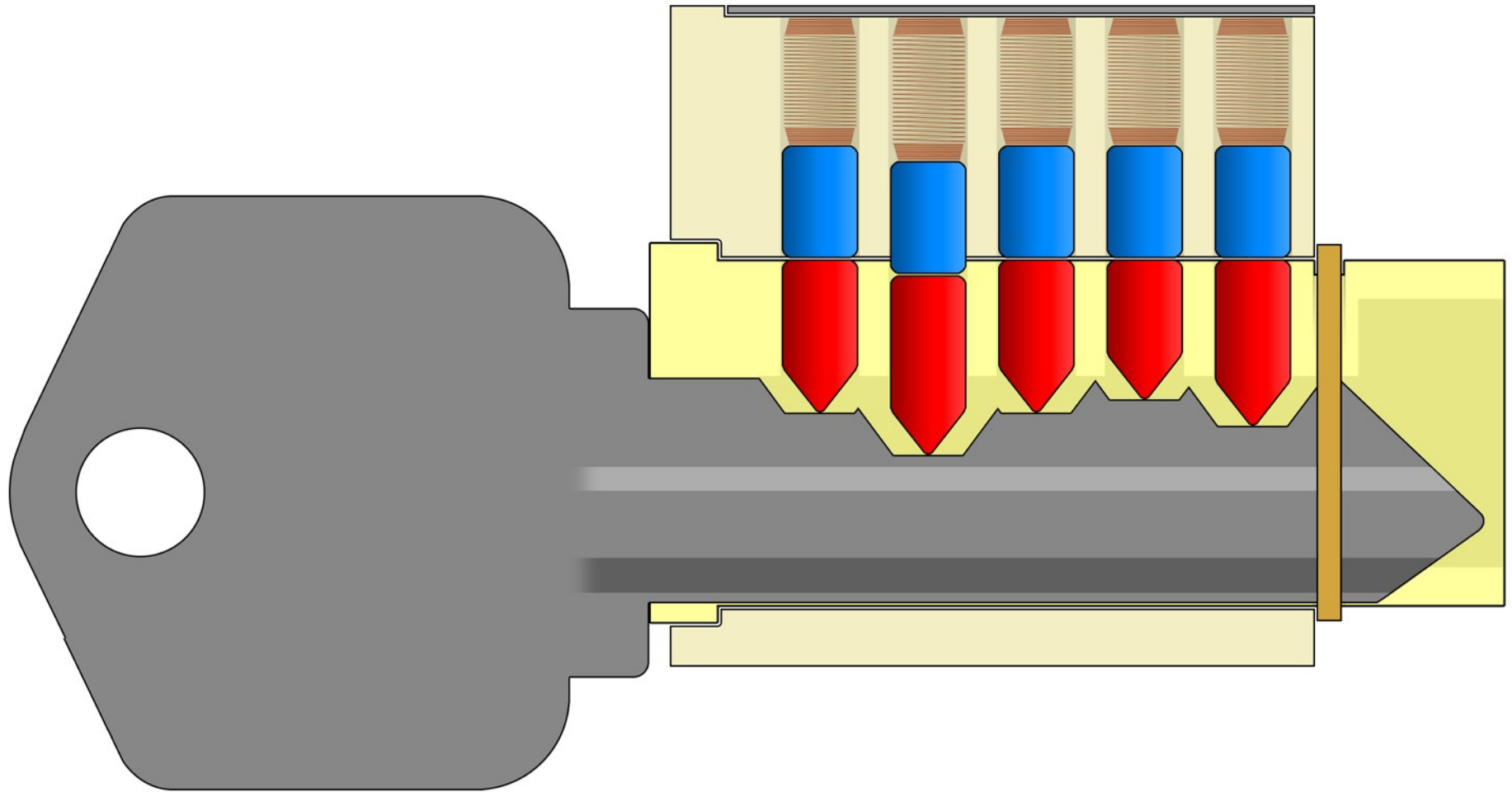
It's Not Just a Single Pin Stack



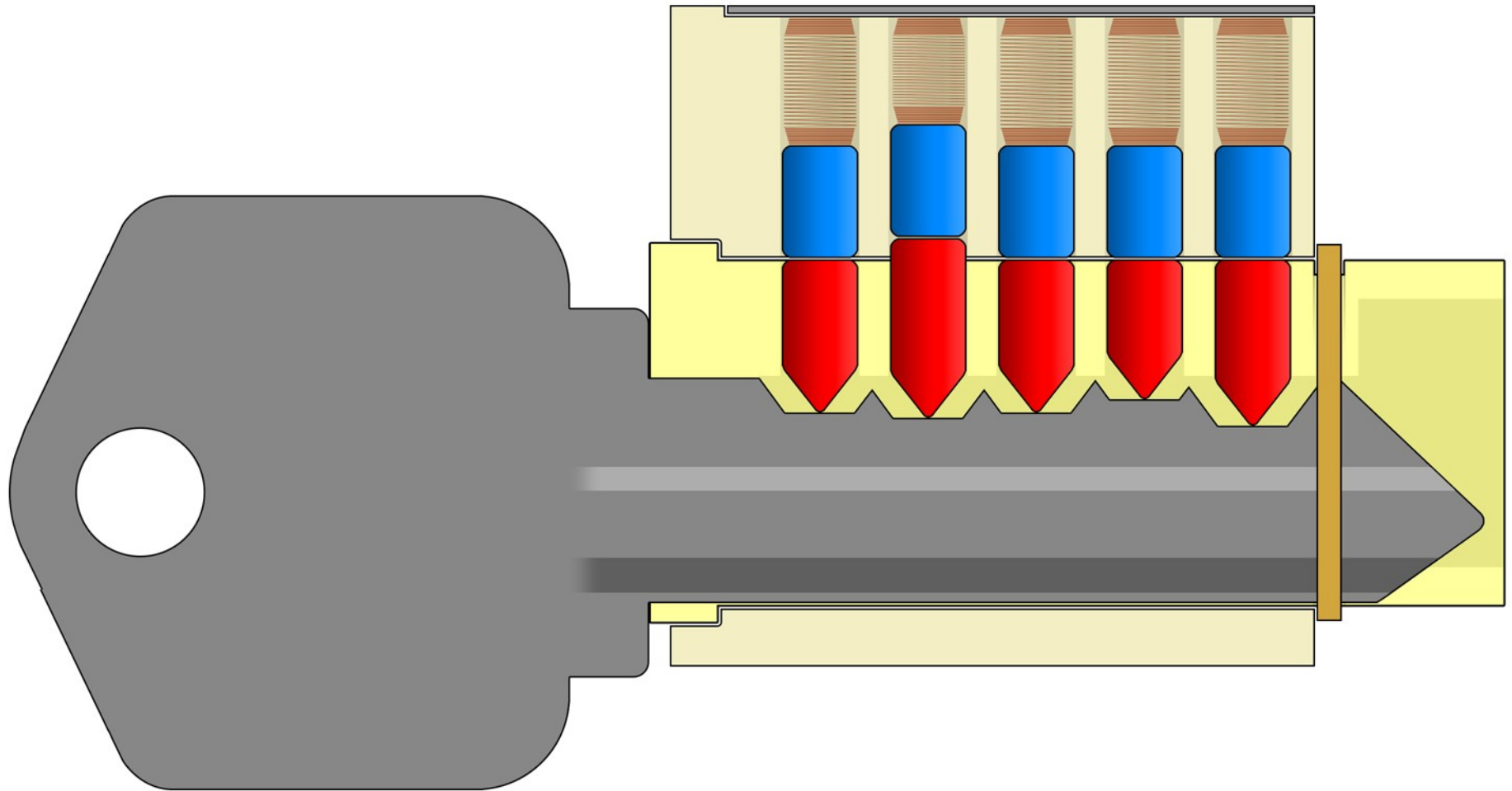
It's Not Just a Single Pin Stack



The Key Has To Be Just Right



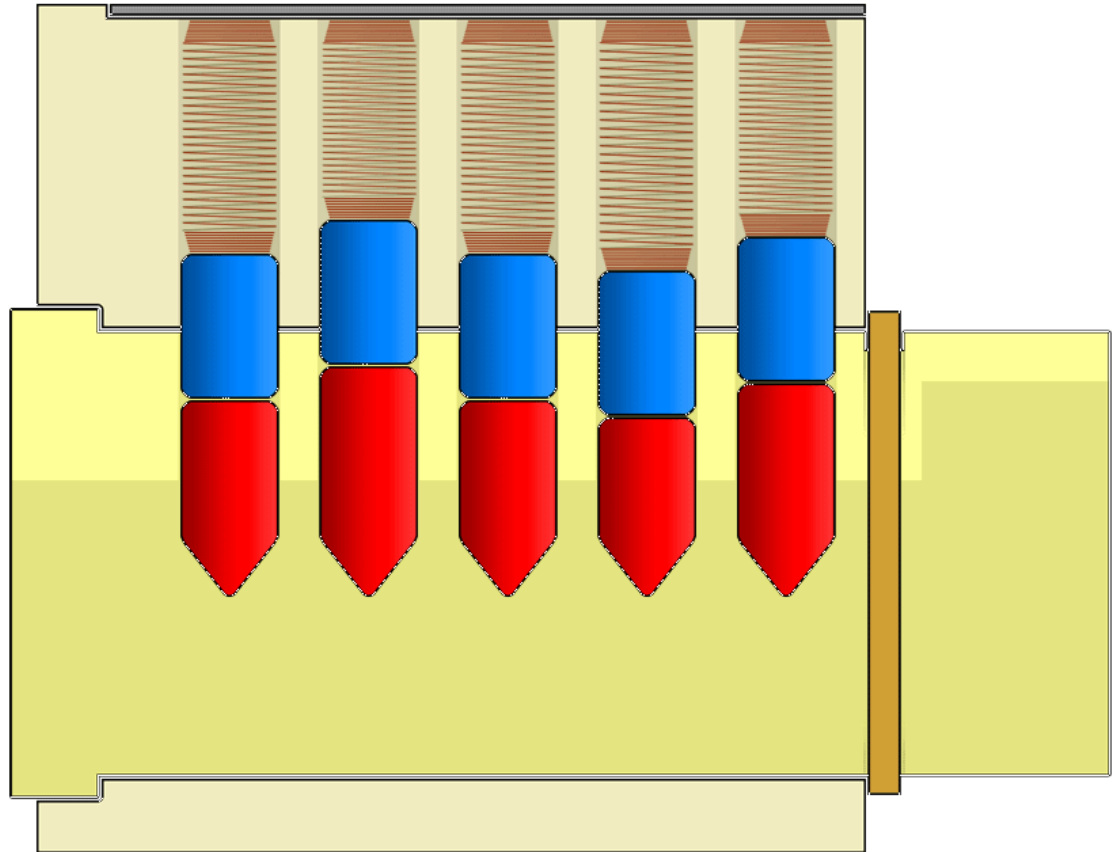
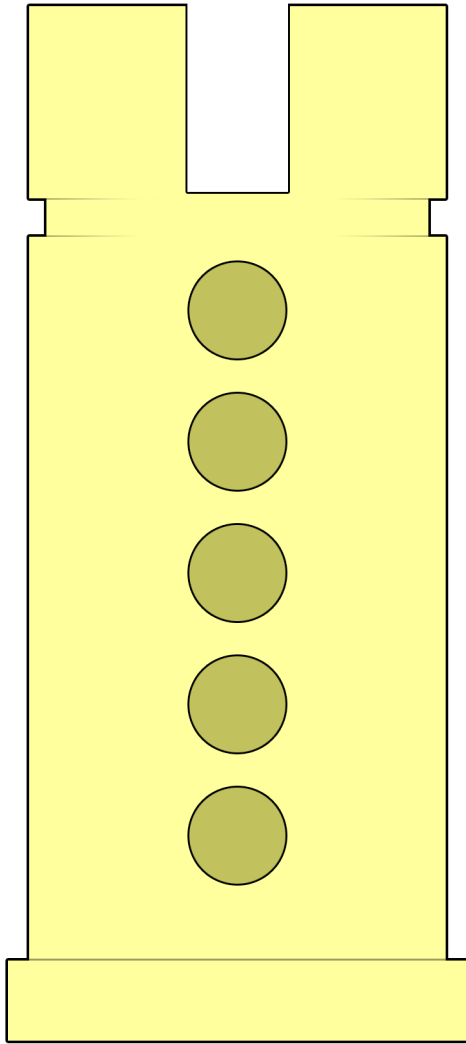
The Key Has To Be Just Right



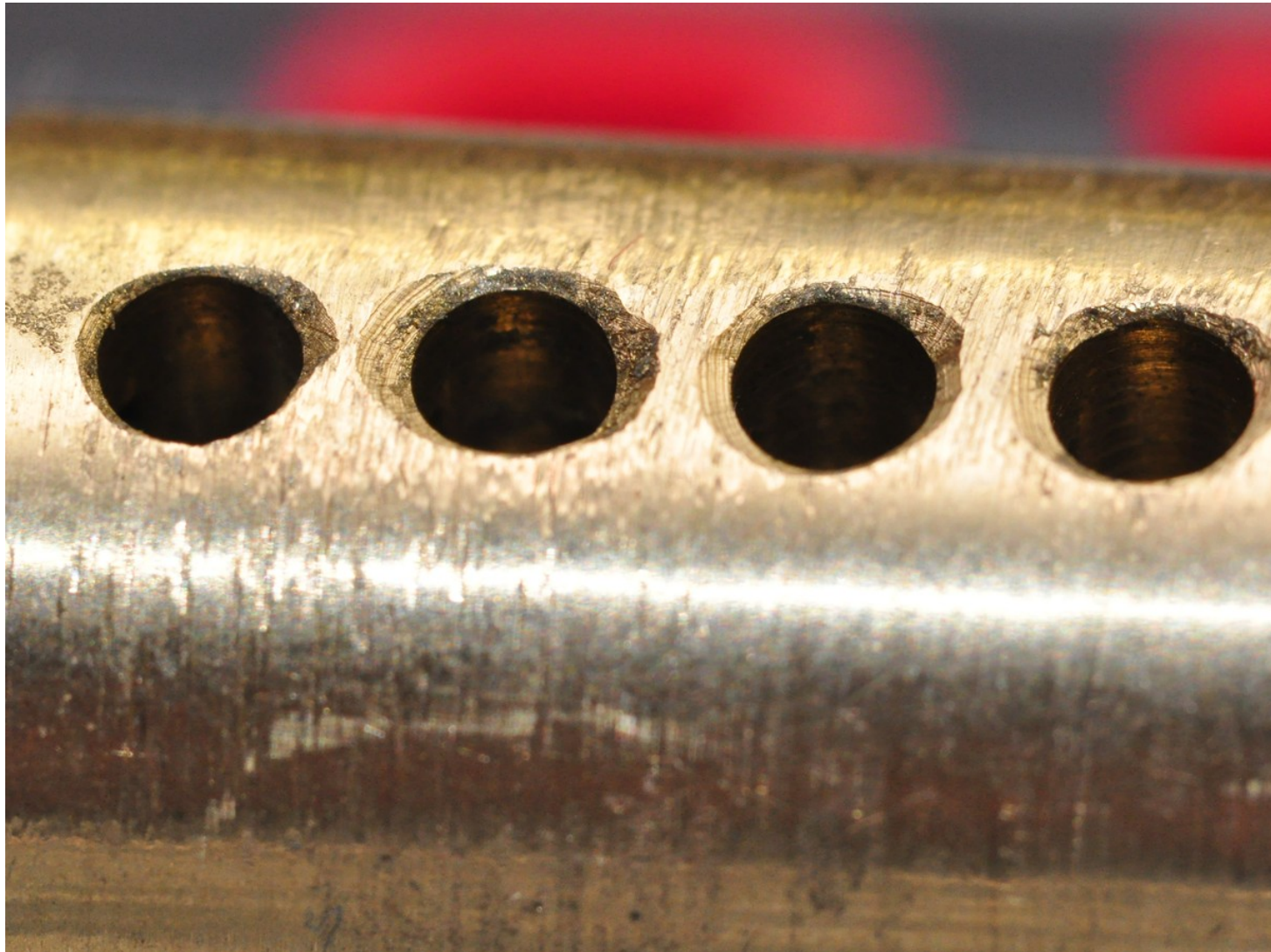
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. **Picking is simple and fun**

In An Ideal World ...



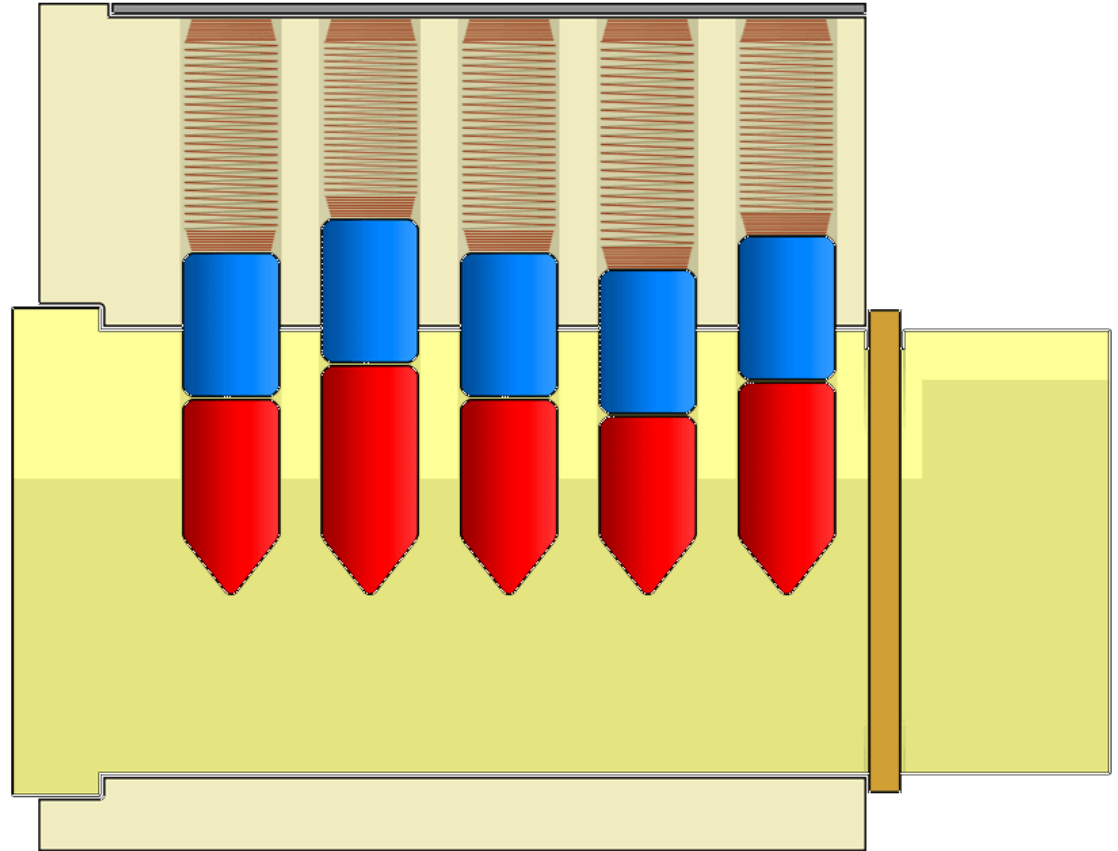
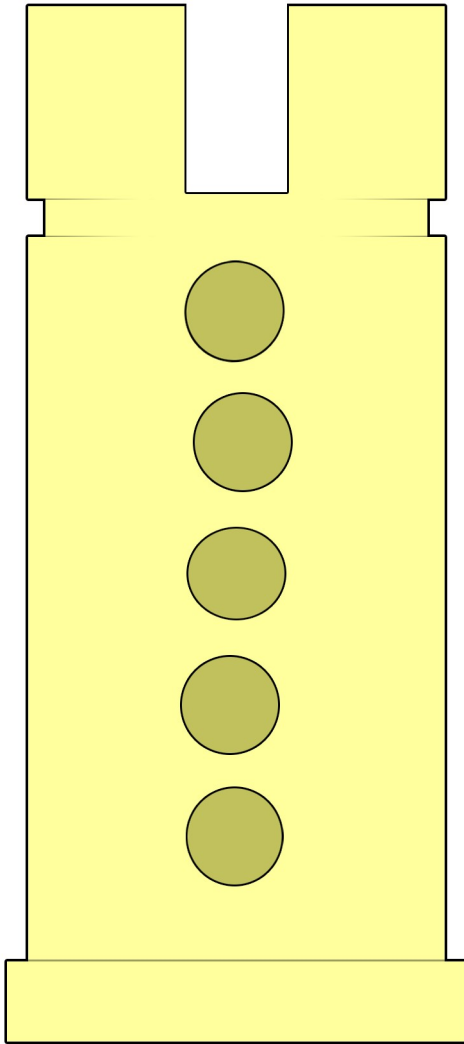
In The Real World ...



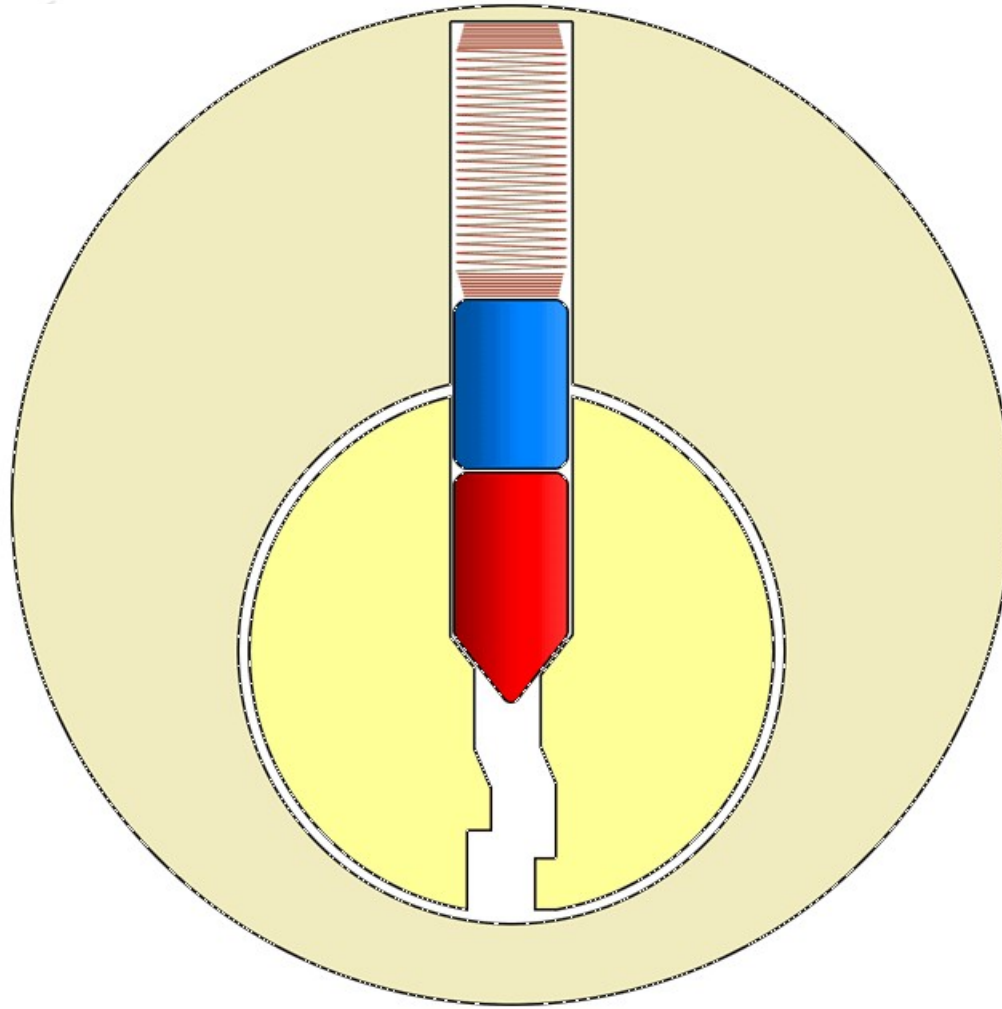
In The Real World ...



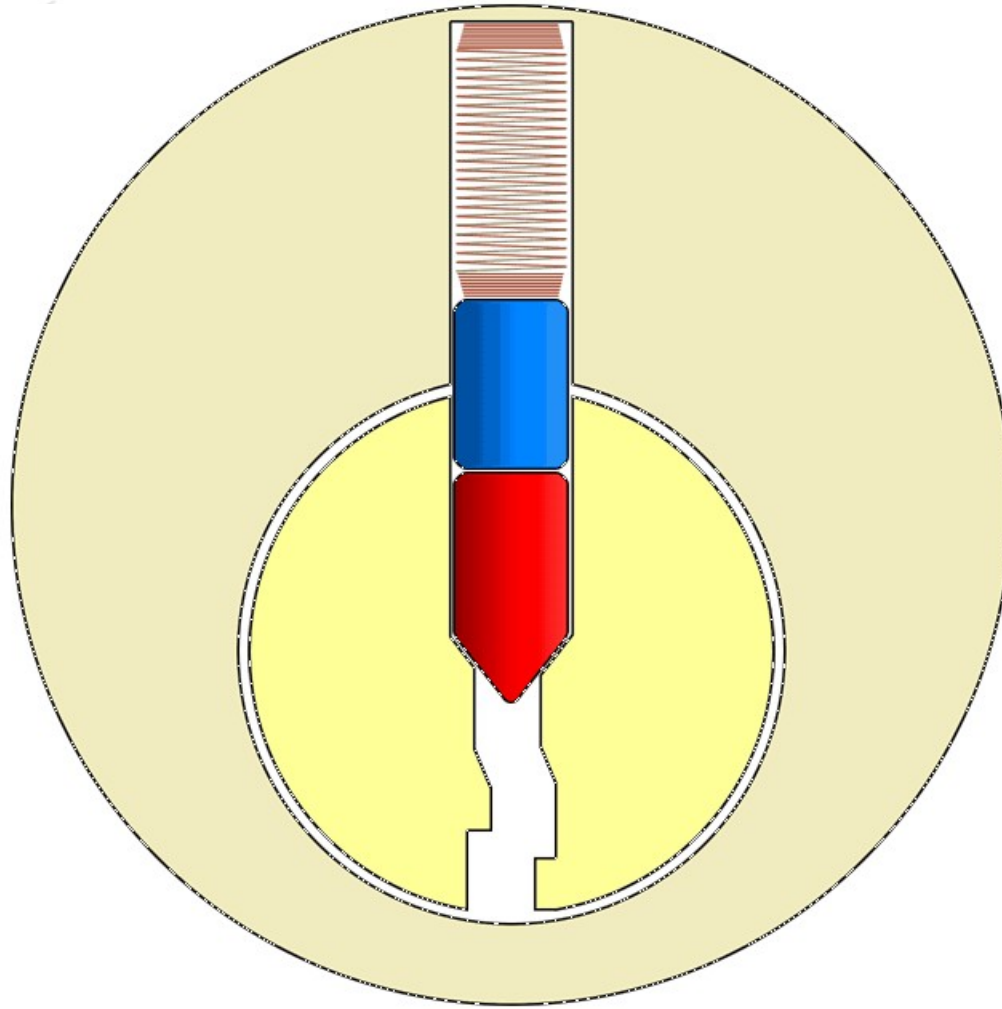
In The Real World ...



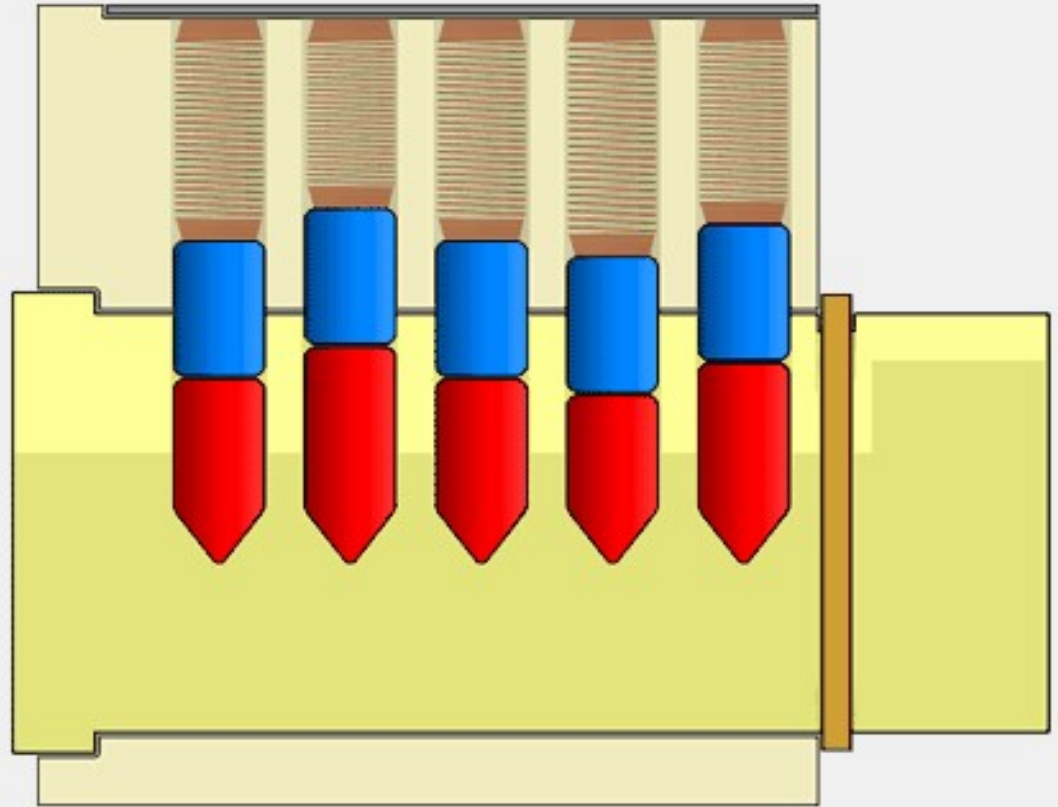
Setting a Pin



Setting a Pin



Setting the Pins



Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement

Other Ways of Arranging the Pins



Other Ways of Attacking the Pins



A Fun Tubular Lock Story



A Fun Tubular Lock Story



A Fun Tubular Lock Story



A Fun Tubular Lock Story



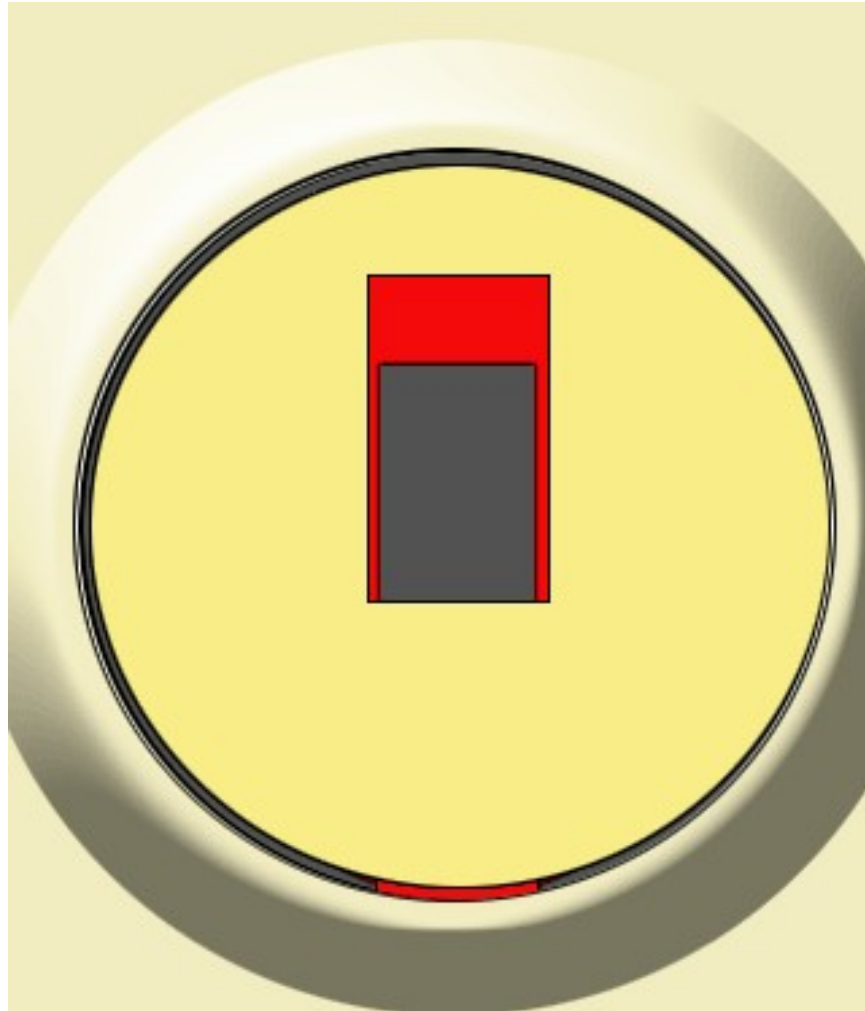
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. **Other everyday designs are often weak, too**

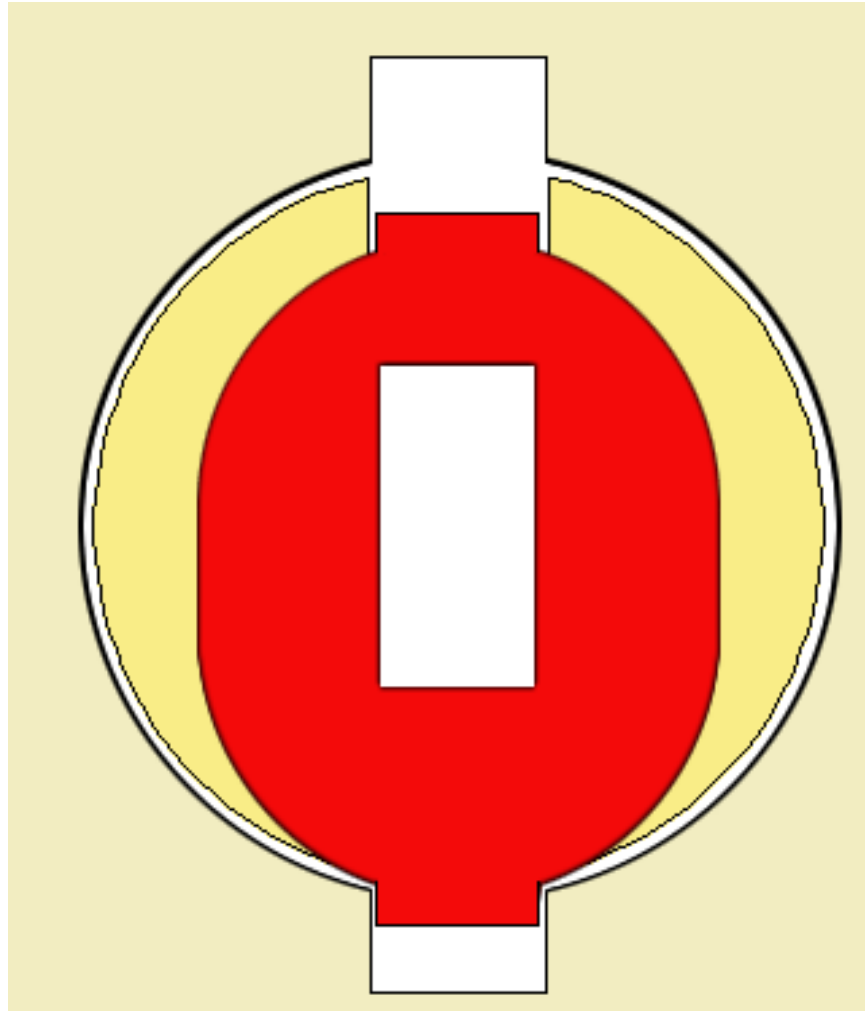
Wafer Locks



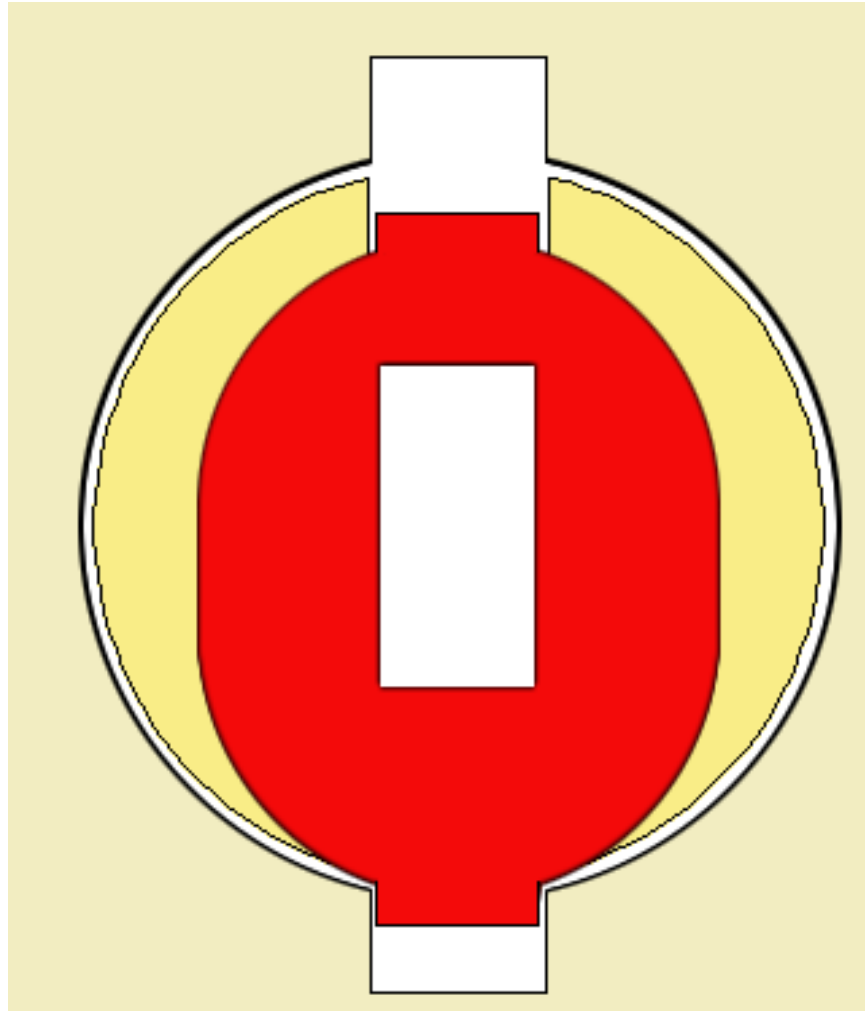
Wafer Locks



Wafer Locks



Wafer Locks



Raking & Jiggling



A wooden desk drawer is shown, filled with various items. On the left side, there are several stacks of papers and envelopes. One envelope is light blue and has "MENTAL CARE" printed on it. In the center, there is a small box of rubber bands and a small box labeled "THE FOUR SEASONS" with a floral design. To the right of the rubber bands is a small blue notepad. Further right, there is a small American flag, a small white card with the text "DESKTOP PASSWORD: new01s87", and a small white card with the text "DESKTOP PASSWORD: new01s87". On the far right, there is a box of Kleenex tissues, a glue stick, and two small boxes of Tic Tac mints. At the bottom of the drawer, there are several pens and pencils, a small American flag, and two small round trinkets.

Wafer Lock Usage



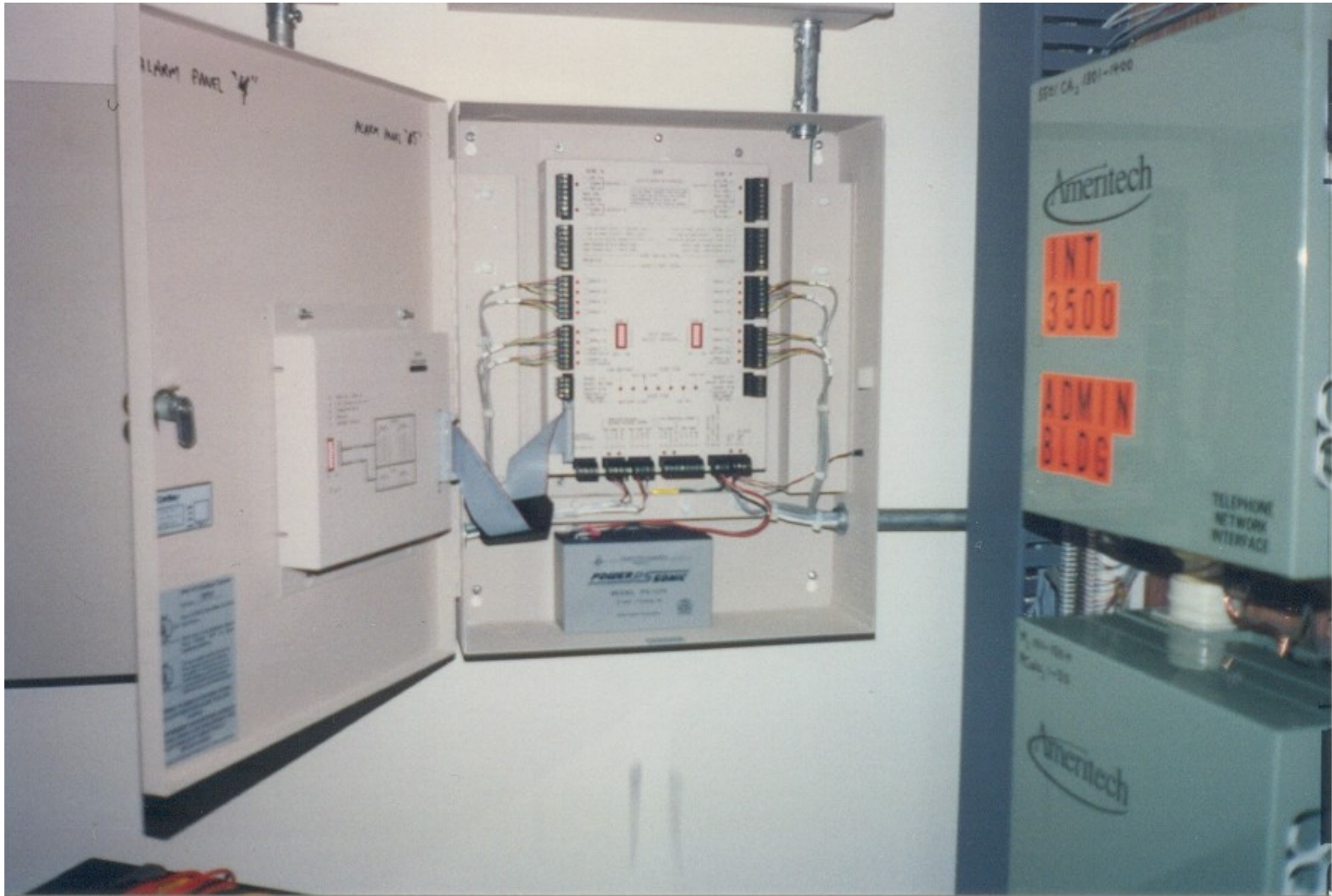
Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



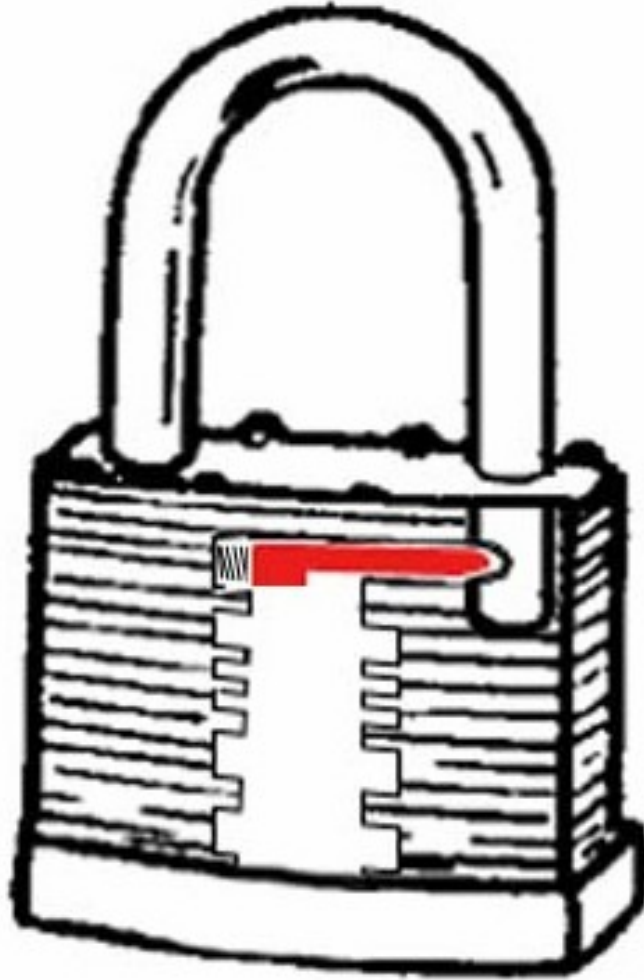
Wafer Lock Usage



Warded Locks



Warded Locks



Warded Locks



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. **You can open locks with beer and beatings**

Popular Padlocks



Terrible Padlocks



Padlock Shims



Padlock Shims... From a Catalog



Padlock Shims... From a Beer Can



Padlock Shims



Padlock Shims



Padlock Shims



Padlock Shims



Padlock Shims



Padlock Shims



Padlock Shim Prevention

Double Ball Mechanism



Padlock Shim Prevention

Which Padlocks are Protected?



Padlock Shim Prevention

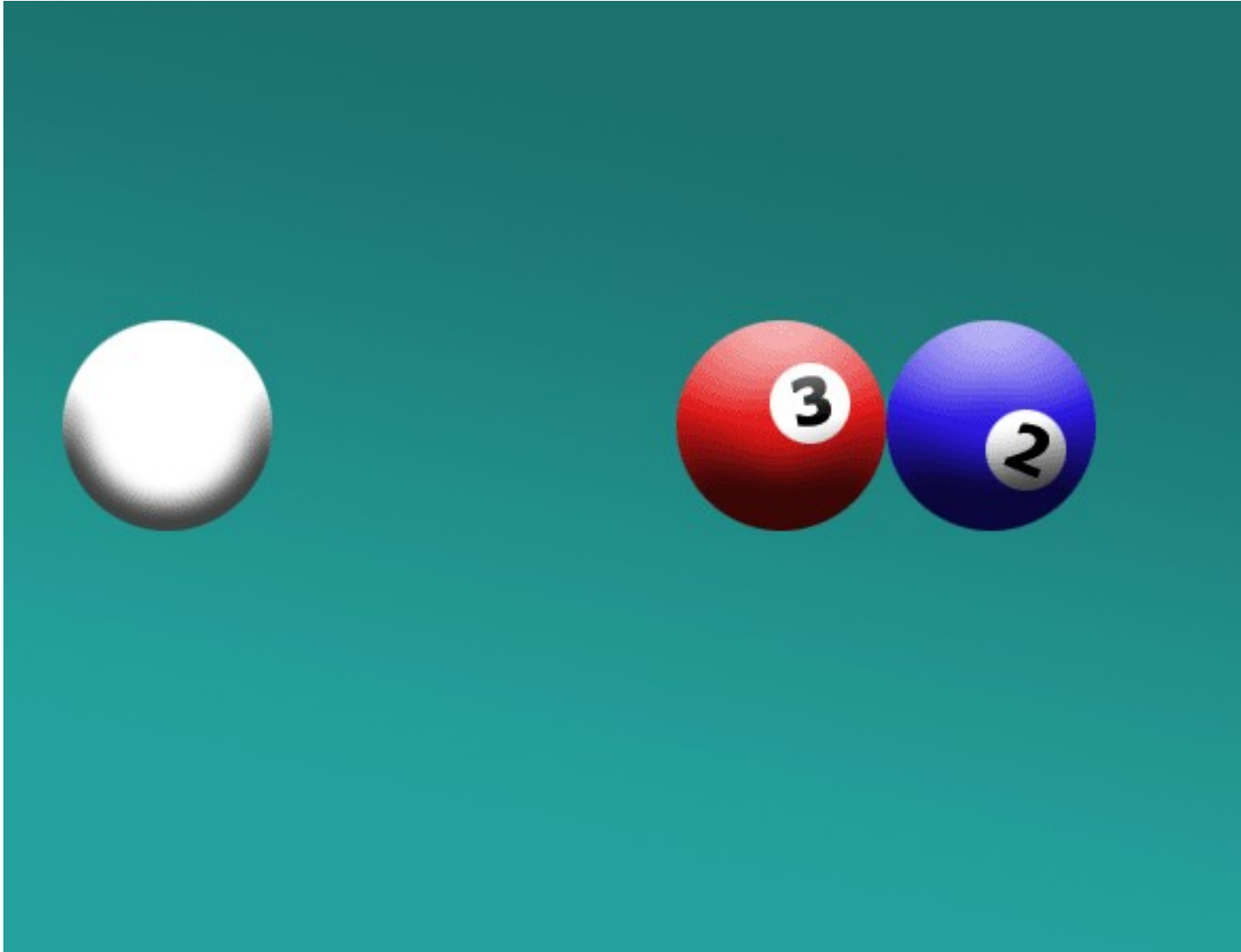


Padlock Shim Prevention

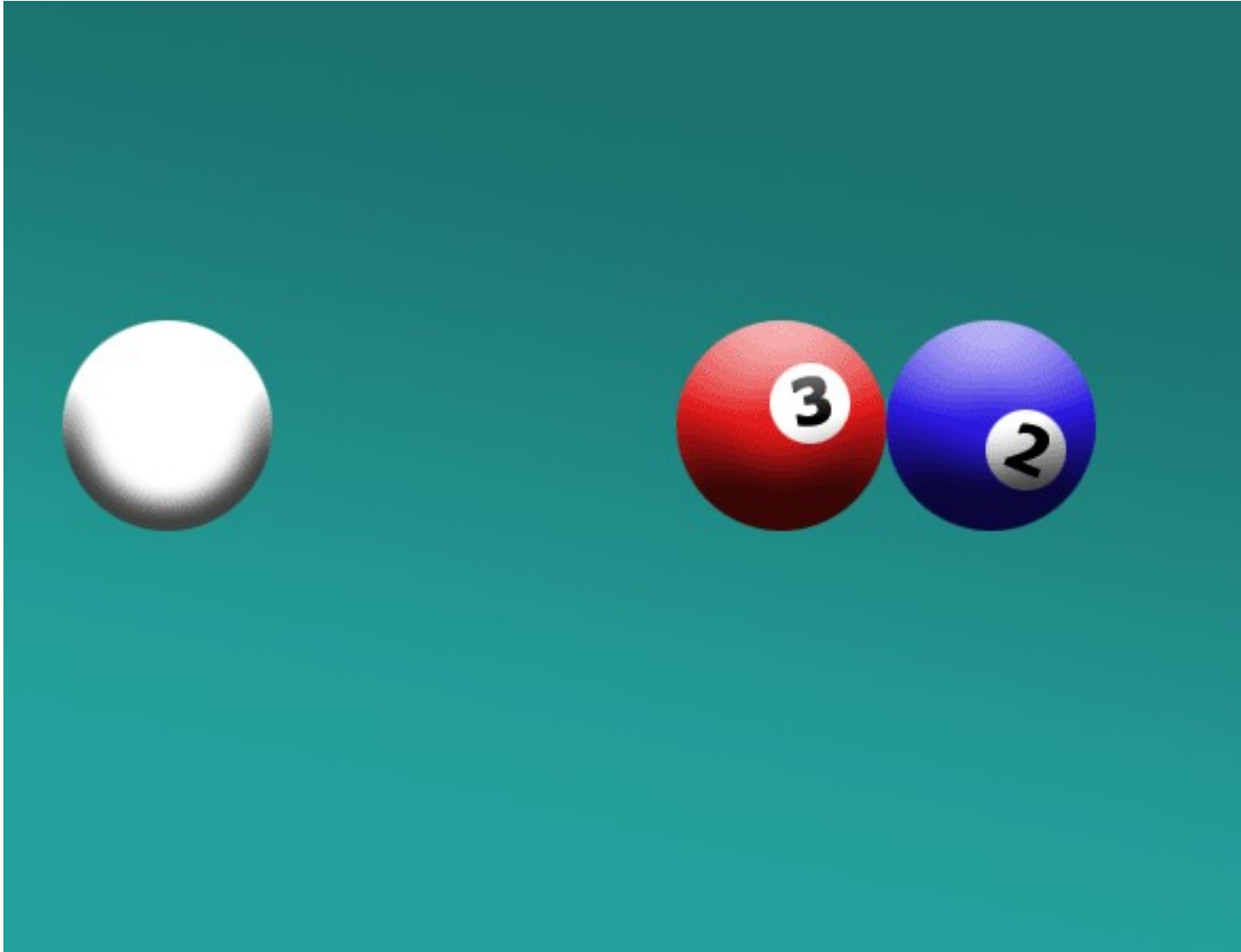


Candado doble traba a bolilla
acero inoxidable

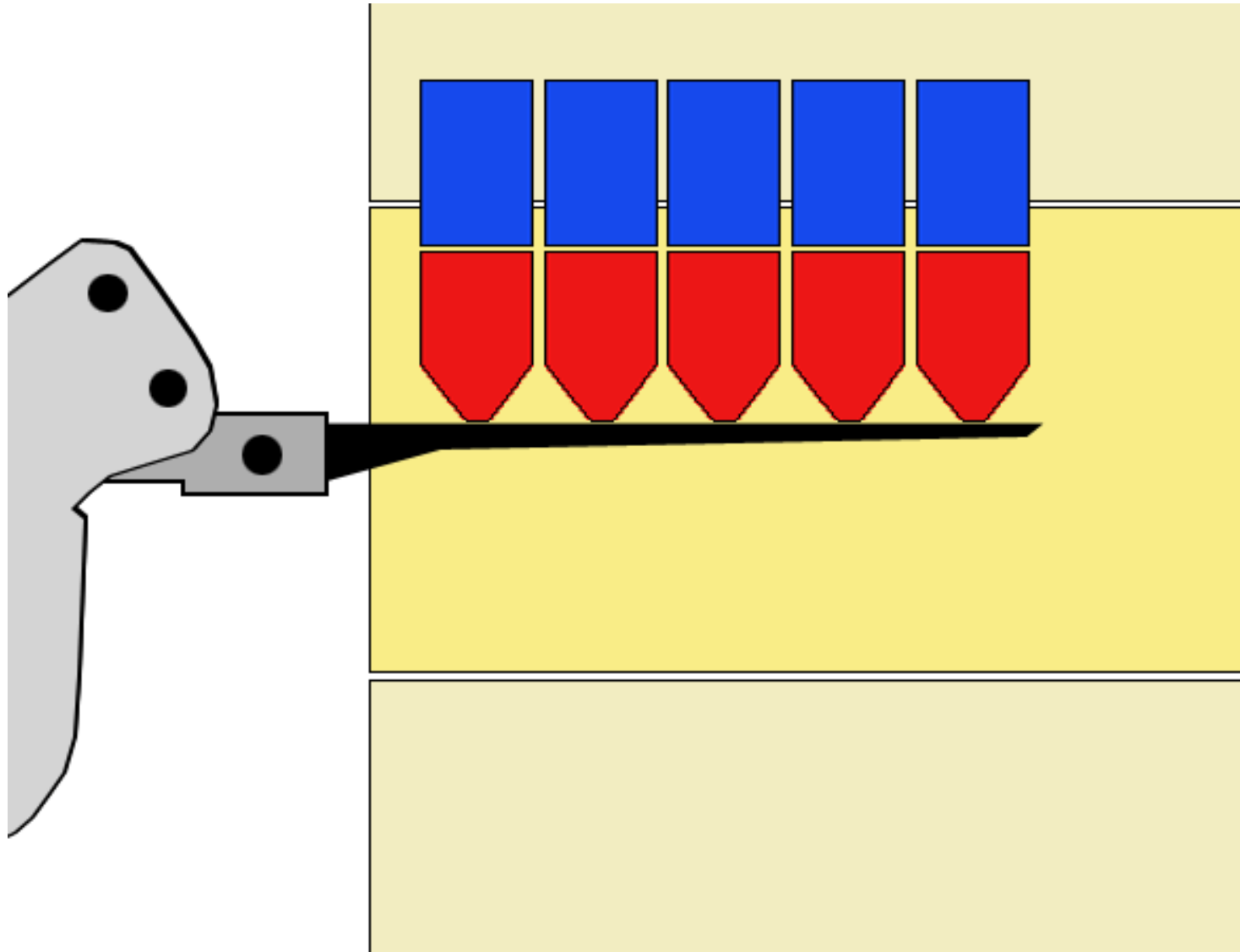
Bumping



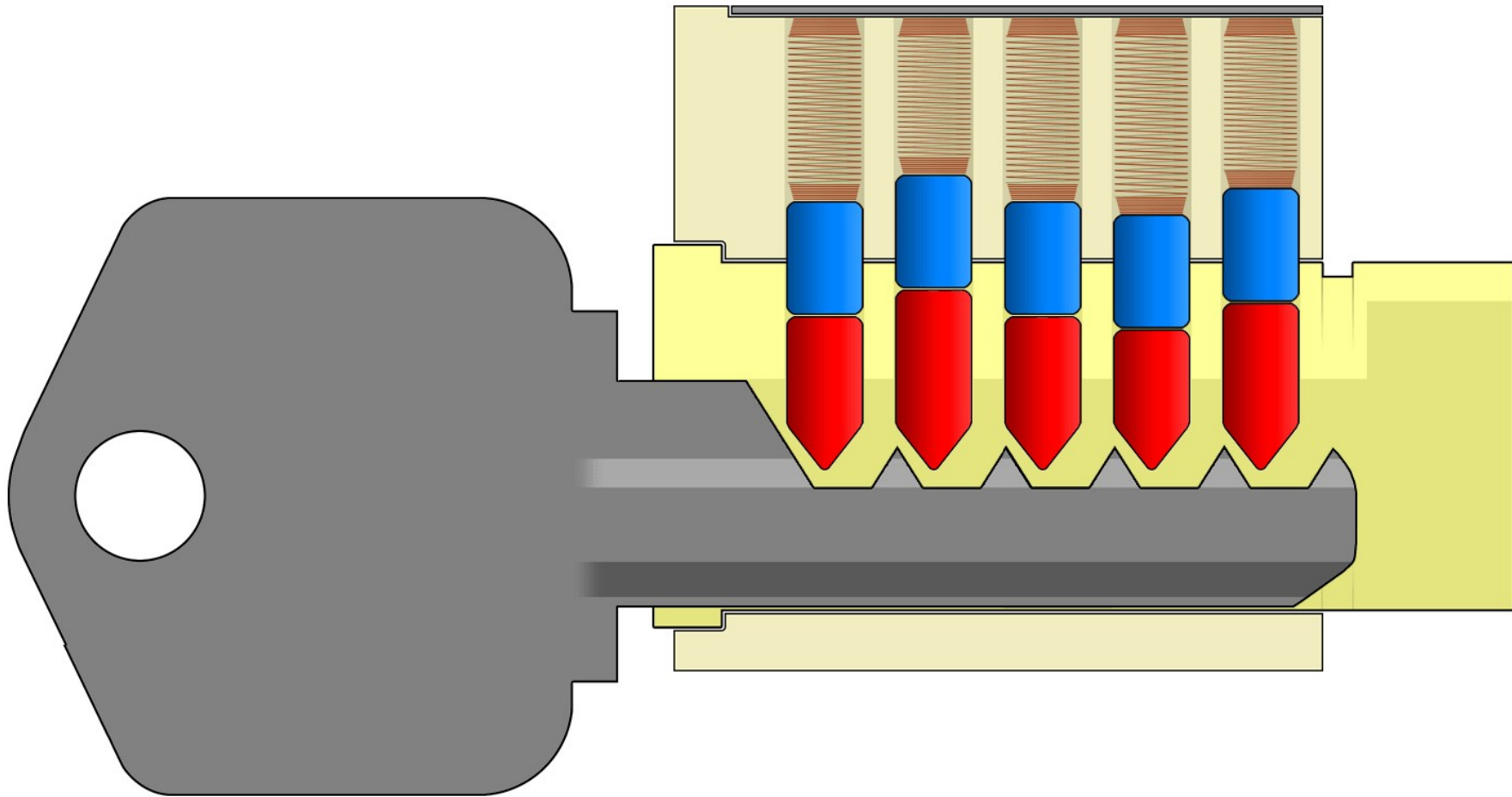
Bumping



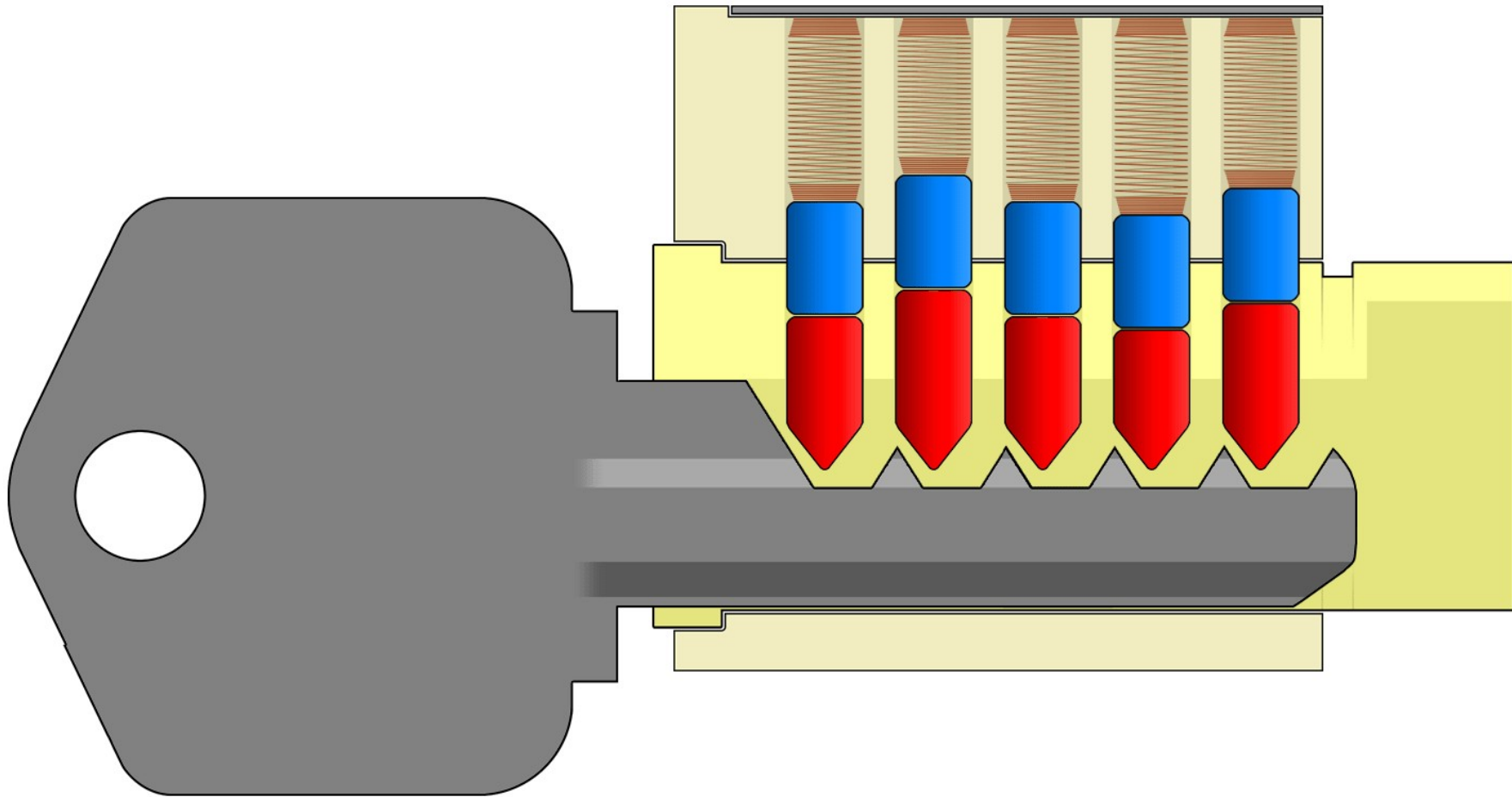
Bumping



Bumping



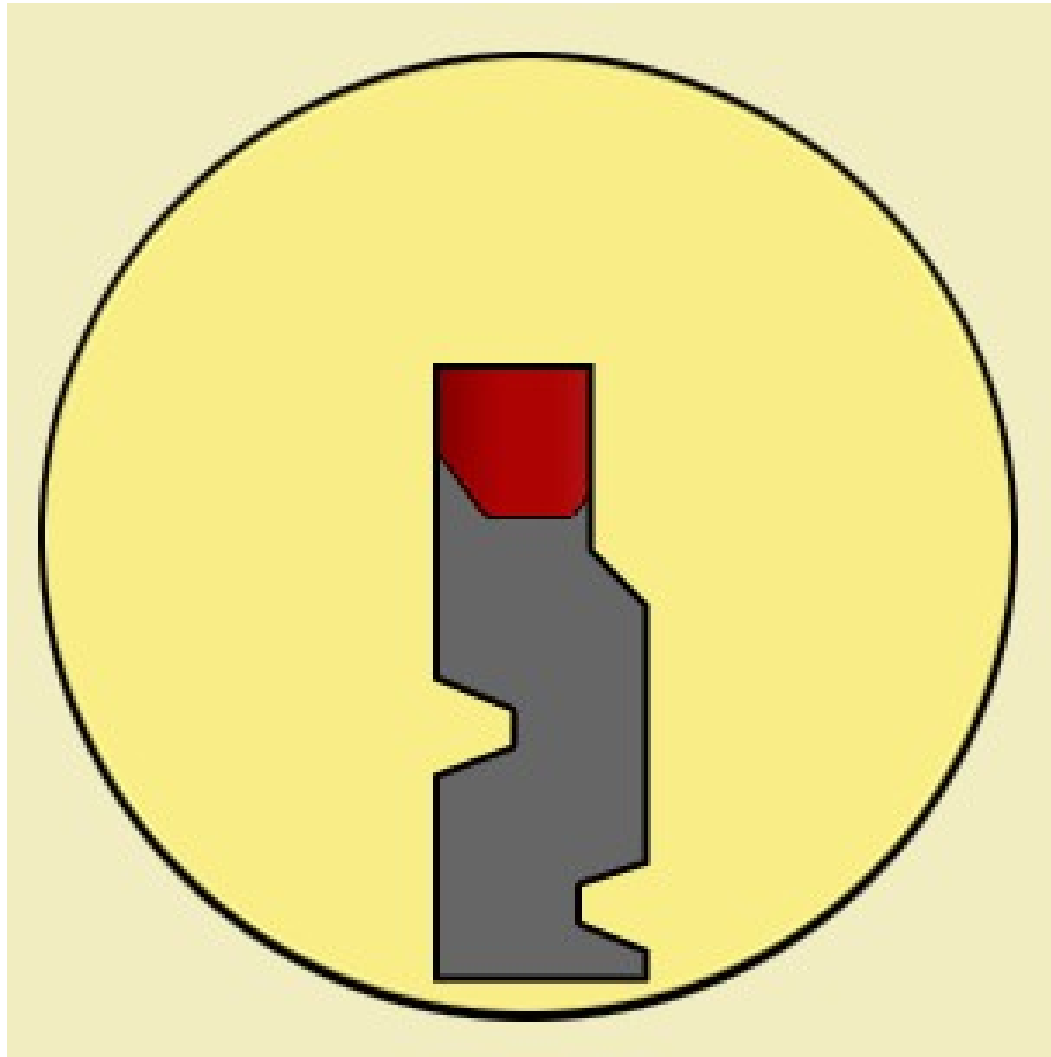
Bumping



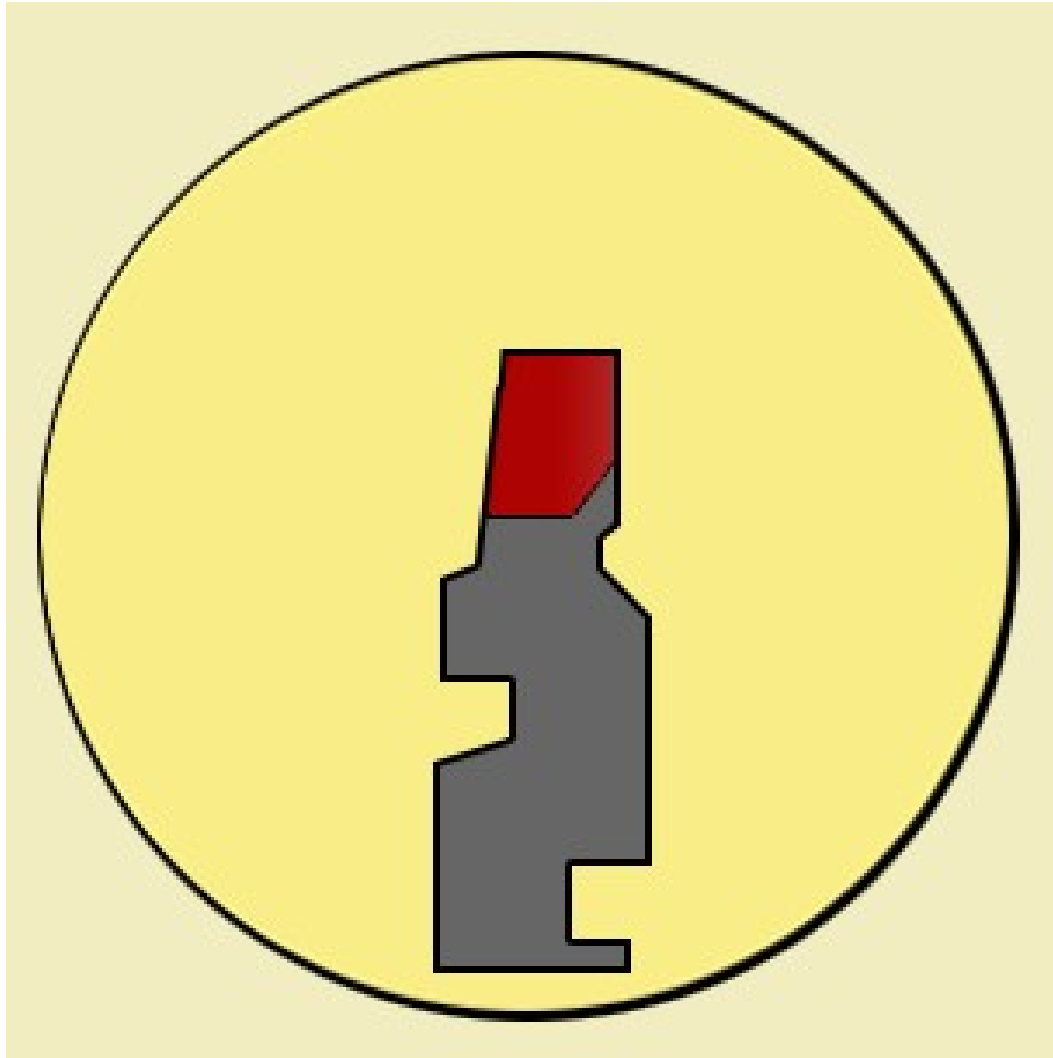
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings

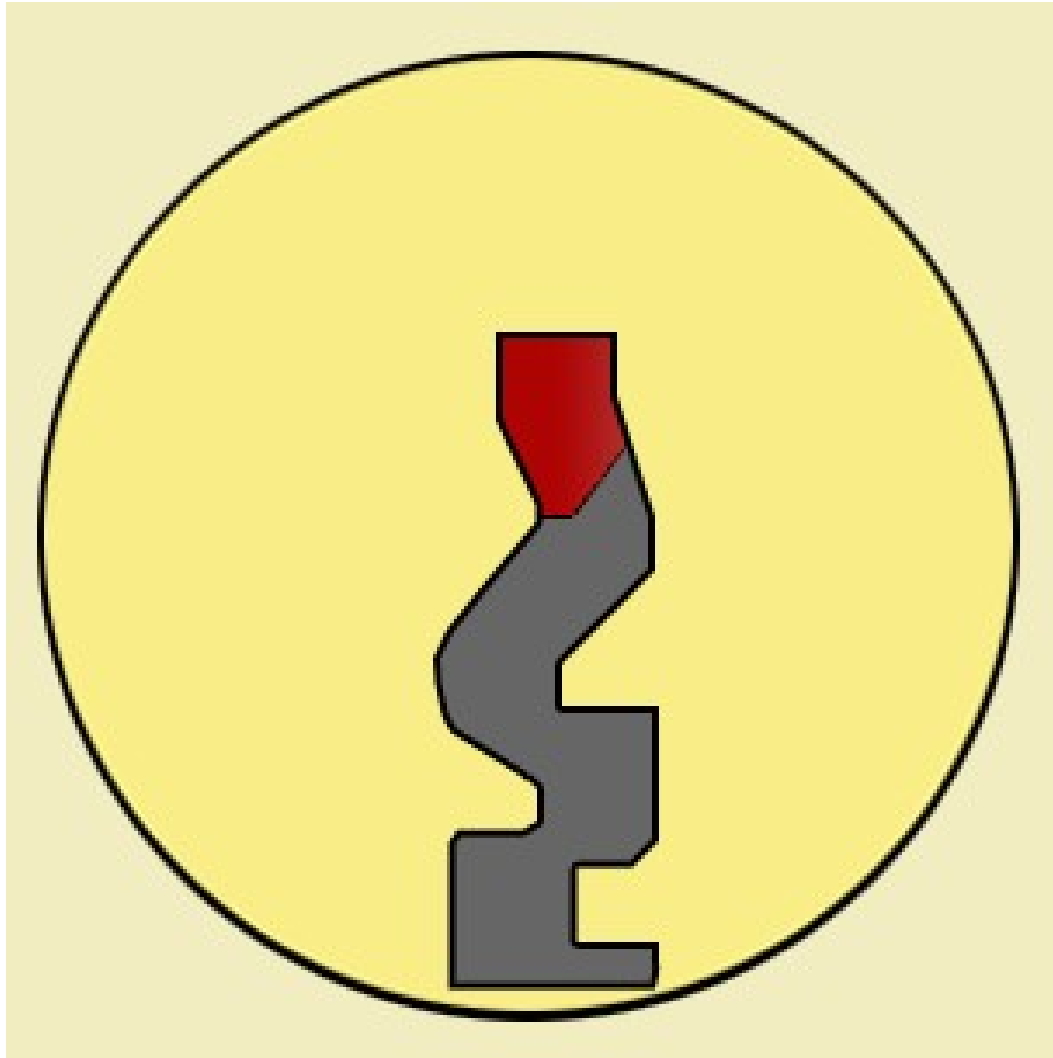
Pick-Resistant Keyways



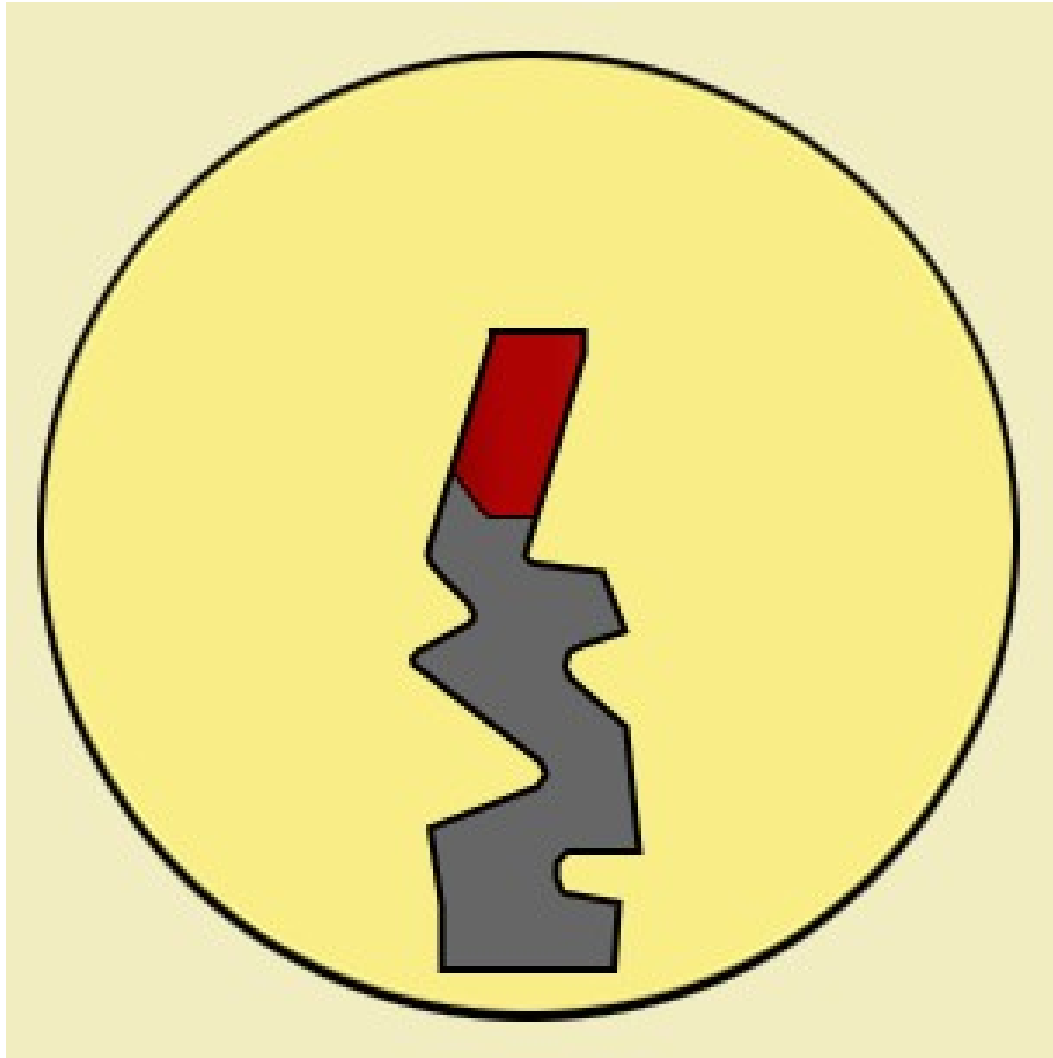
Pick-Resistant Keyways



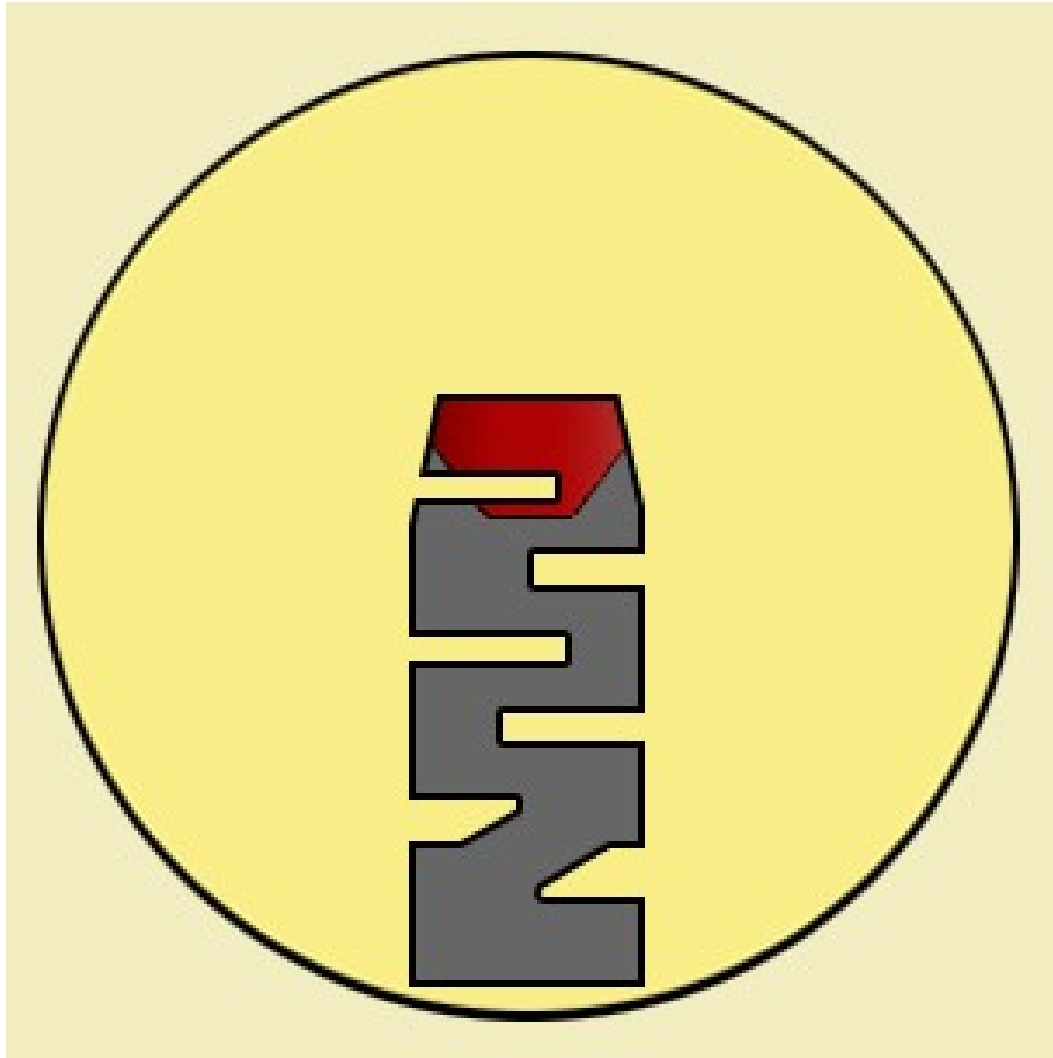
Pick-Resistant Keyways



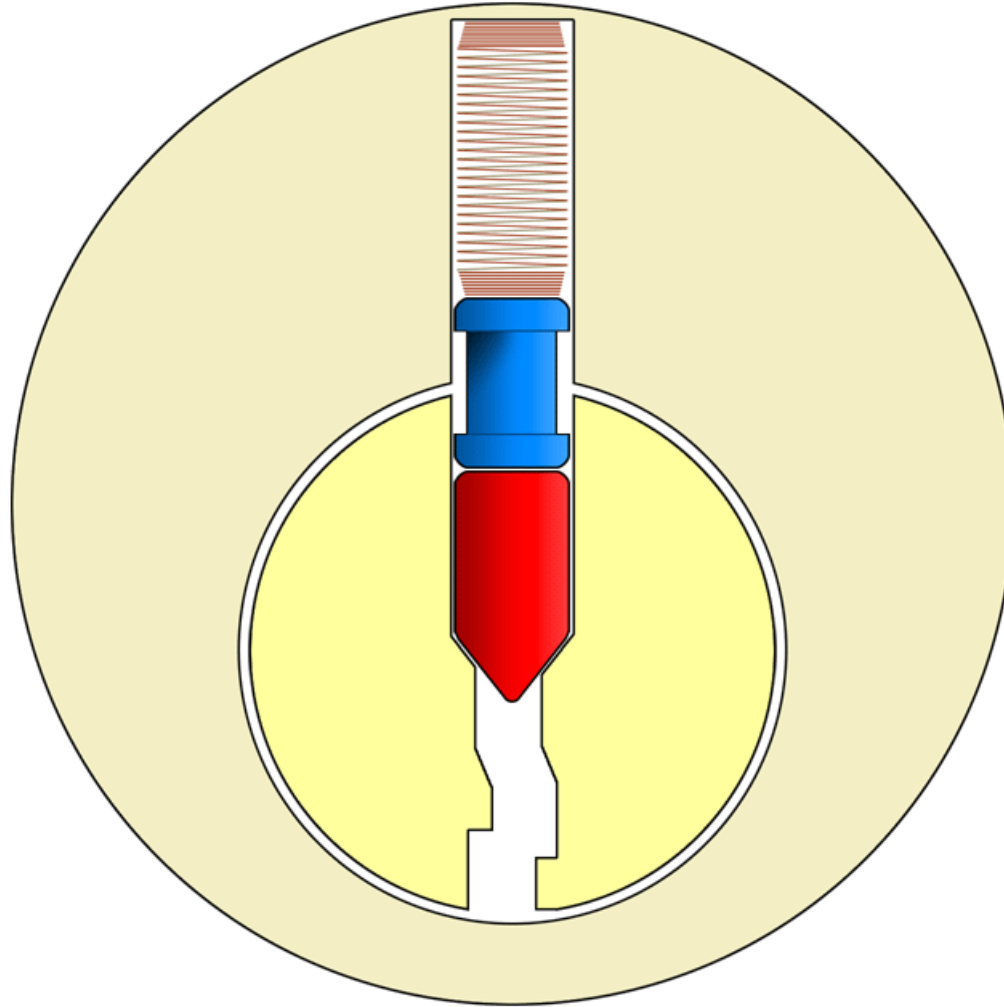
Pick-Resistant Keyways



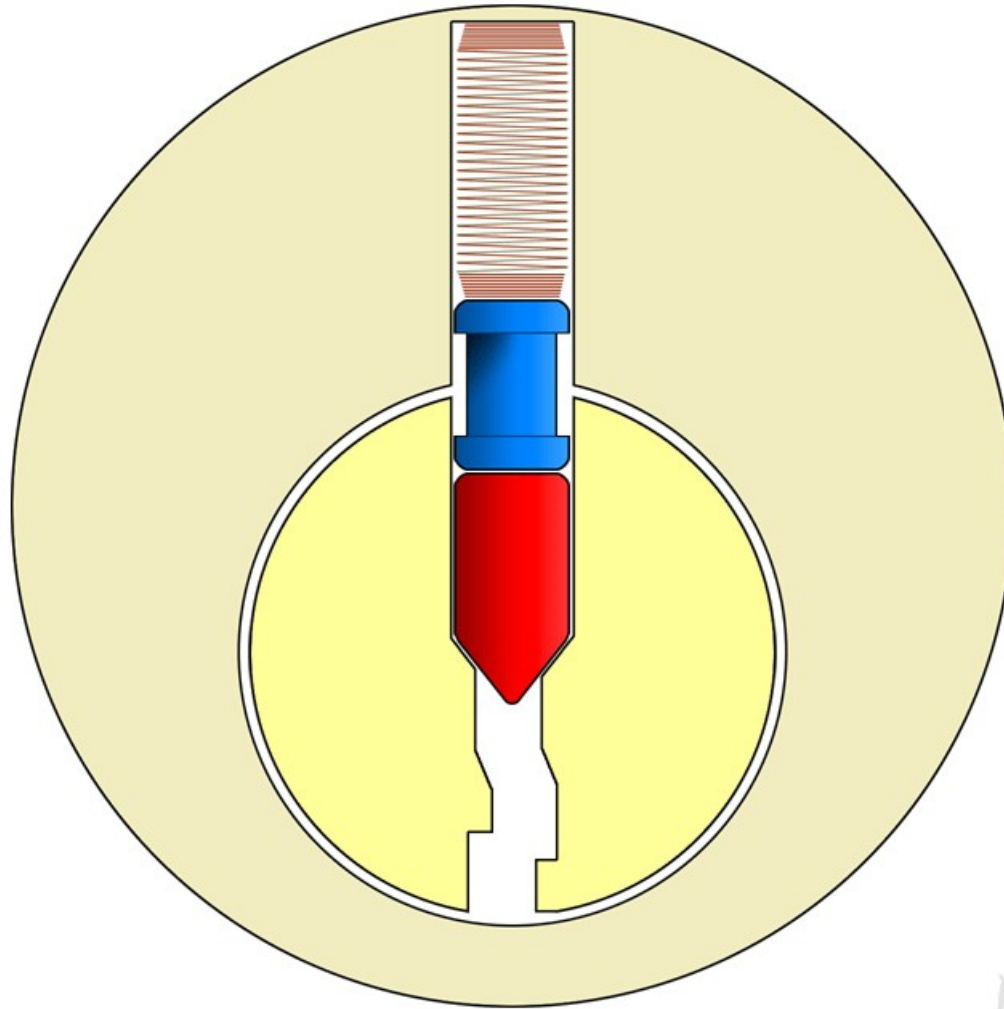
Pick-Resistant Keyways



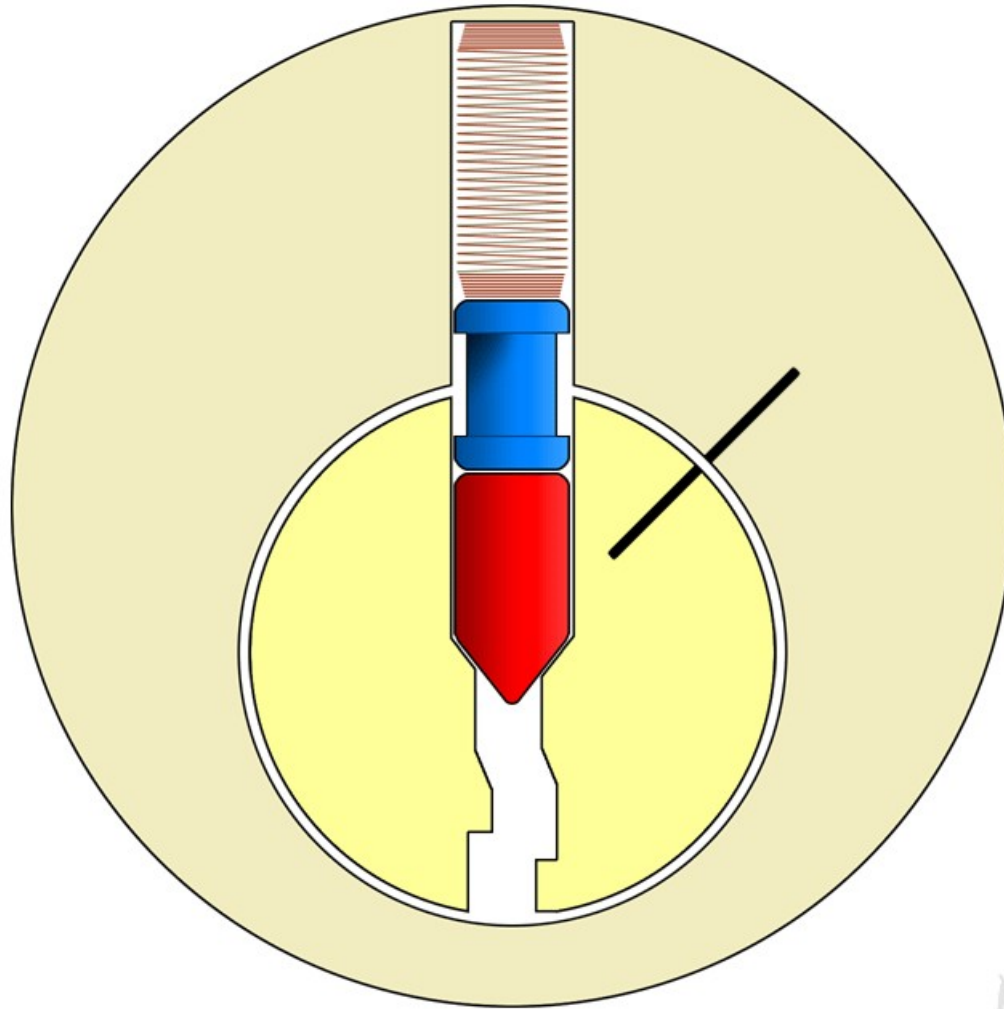
Pick-Resistant Pins



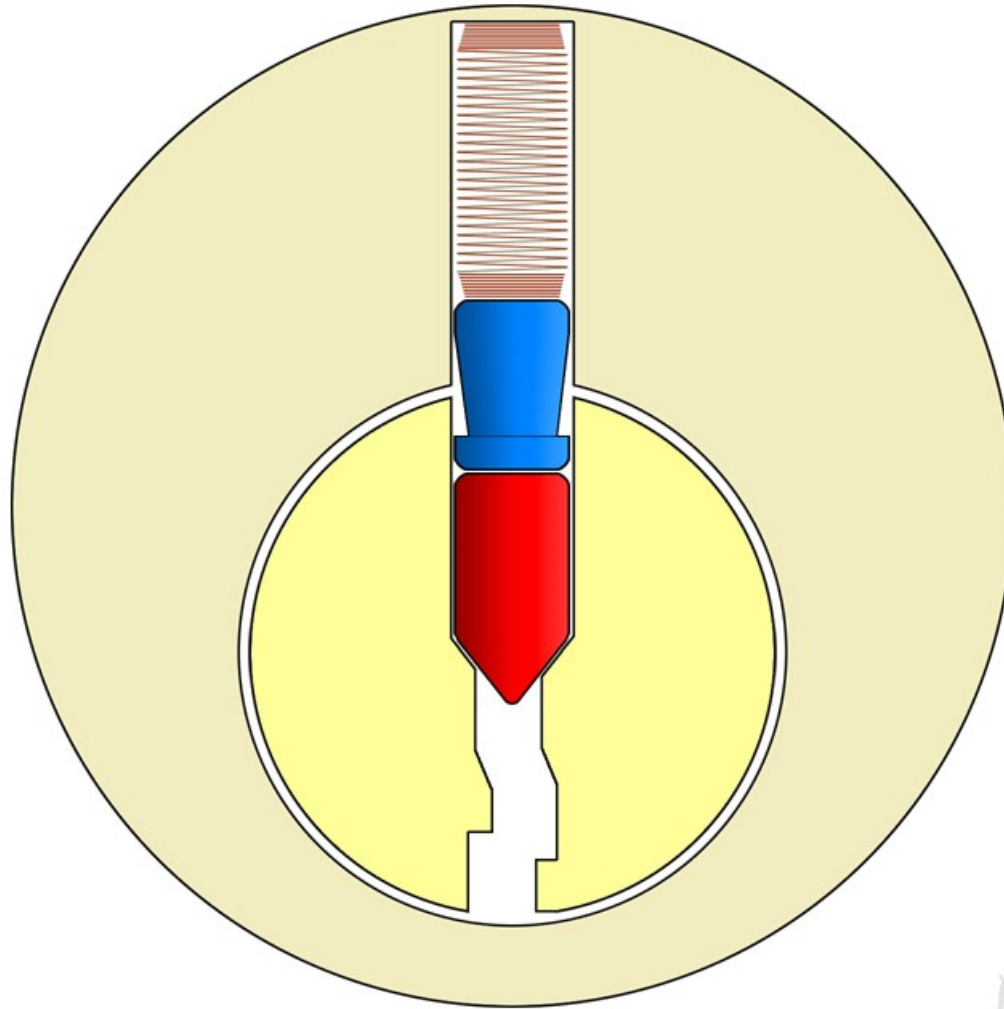
Pick-Resistant Pins



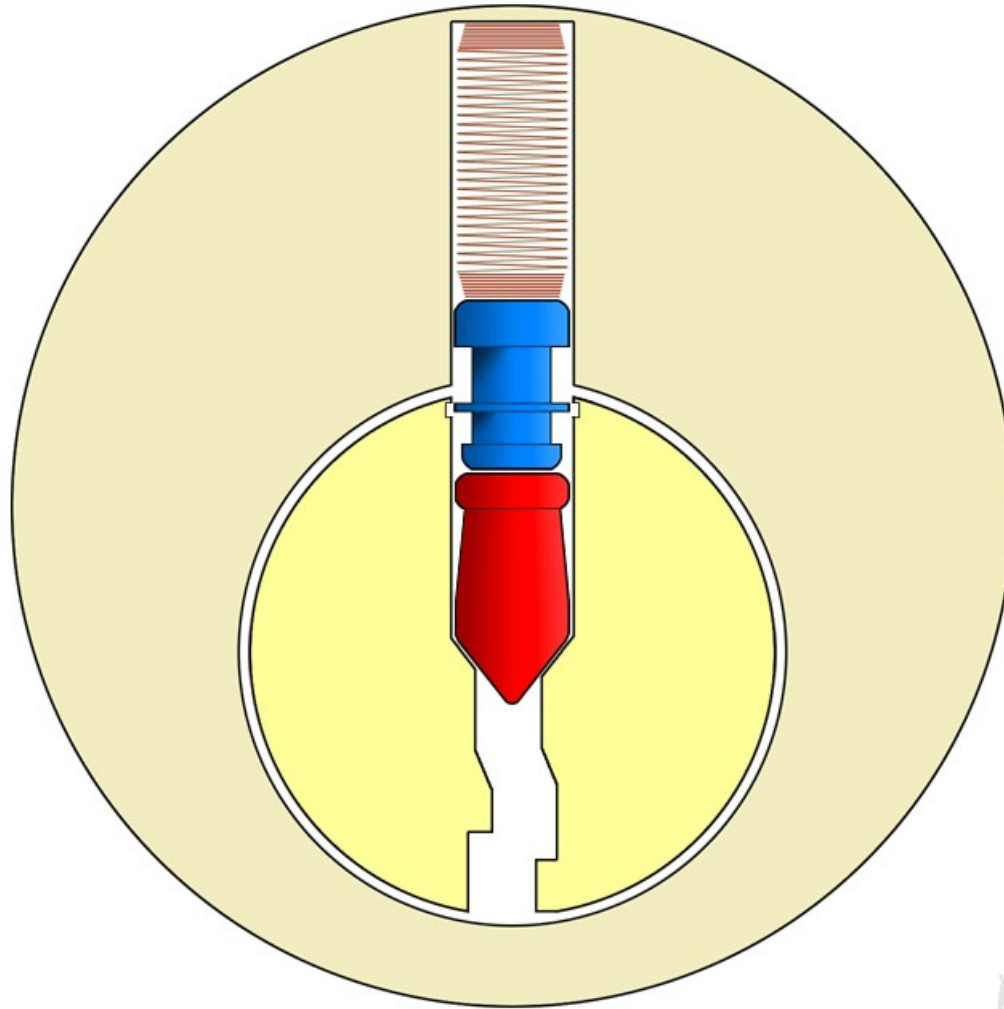
Pick-Resistant Pins



Pick-Resistant Pins



Pick-Resistant Pins



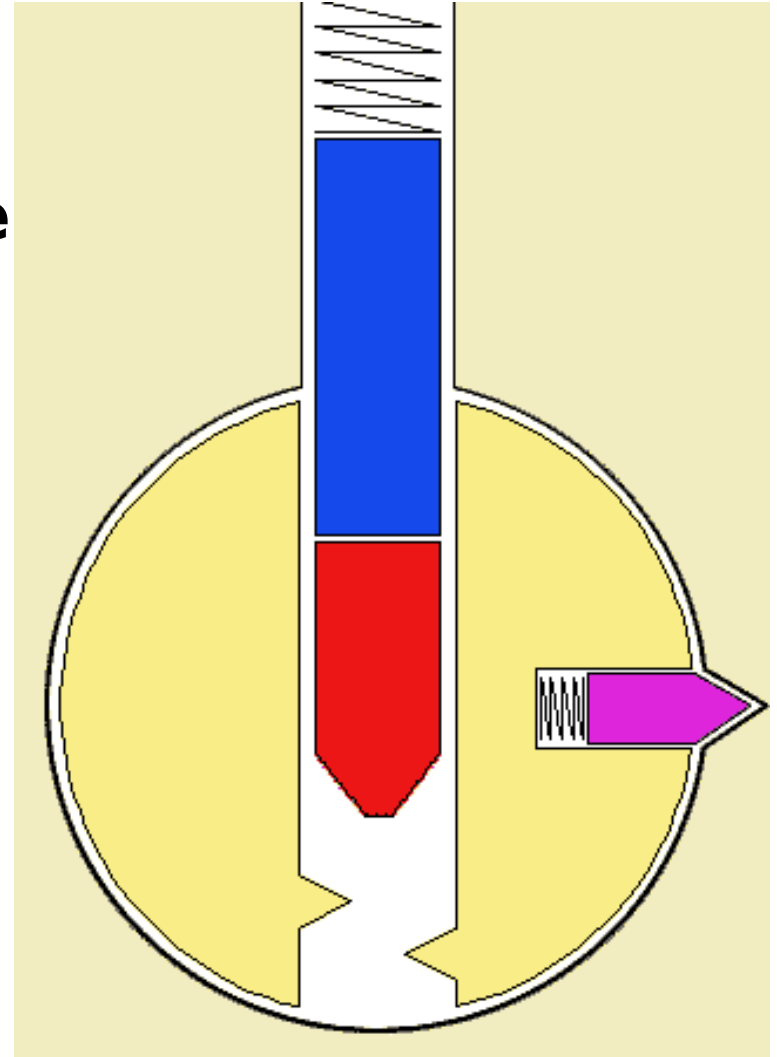
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings



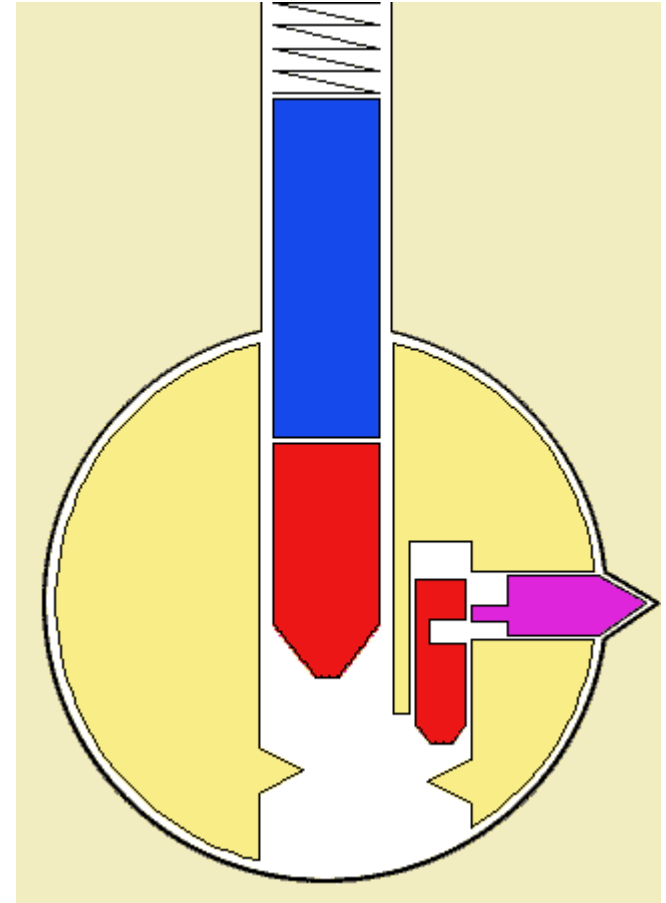
Side Bars

- **Similar to side pins**
- **Restrict plug moveme**
- **Harder to pick than pin stacks**



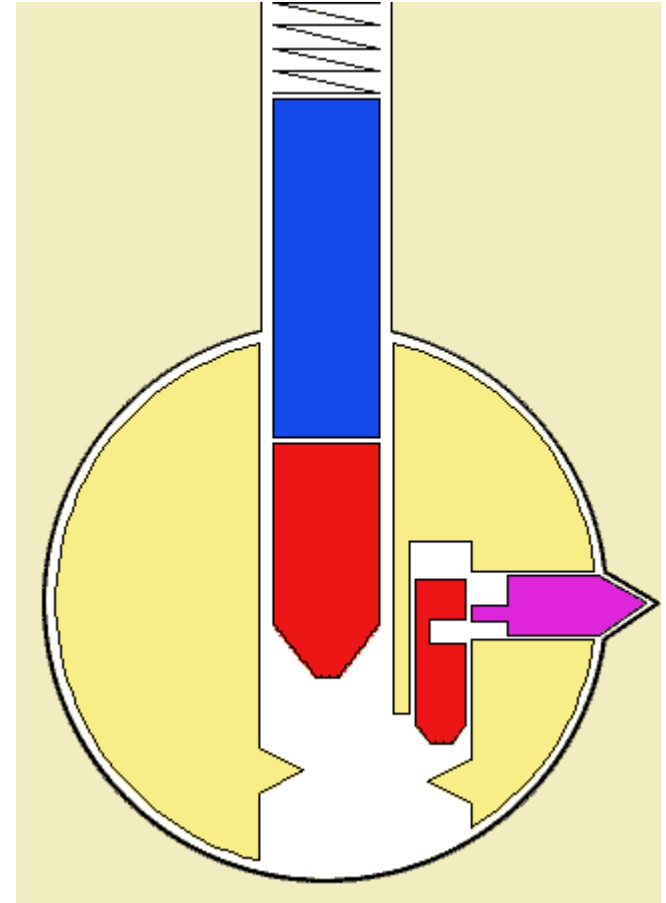
Side Bars

Finger Pins



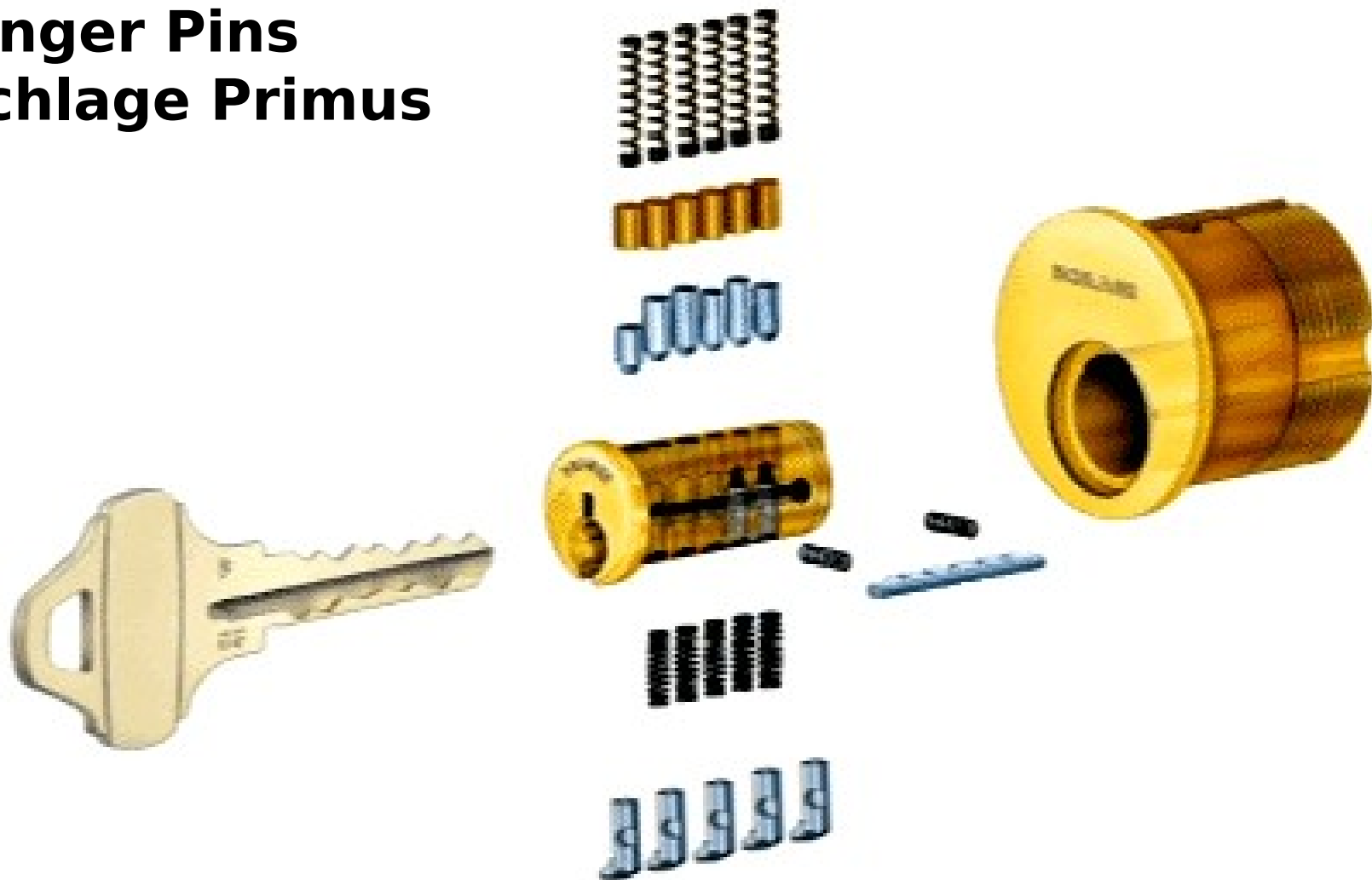
Side Bars

Finger Pins



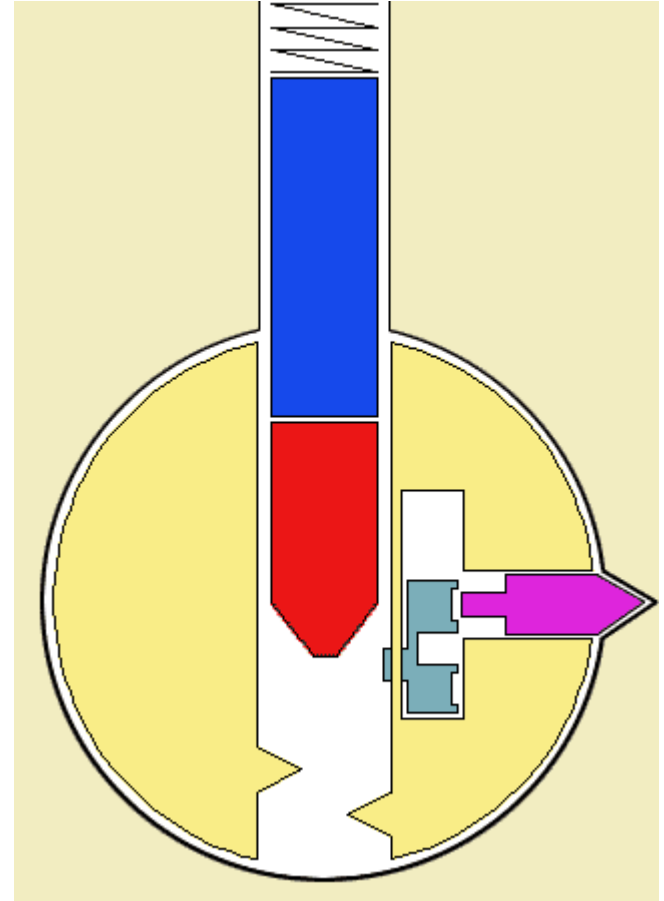
Side Bars

Finger Pins
Schlage Primus



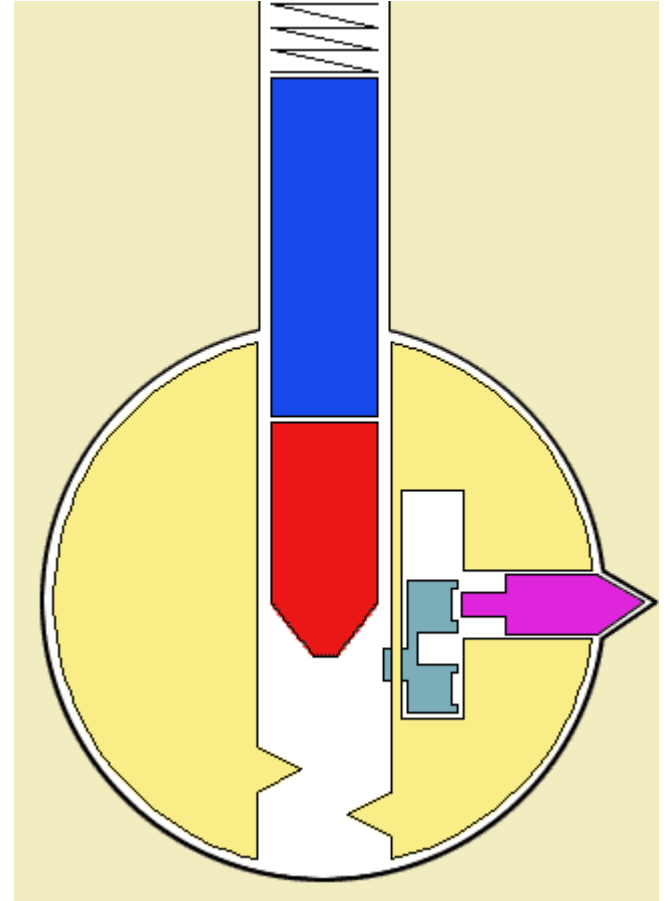
Side Bars

Sliders



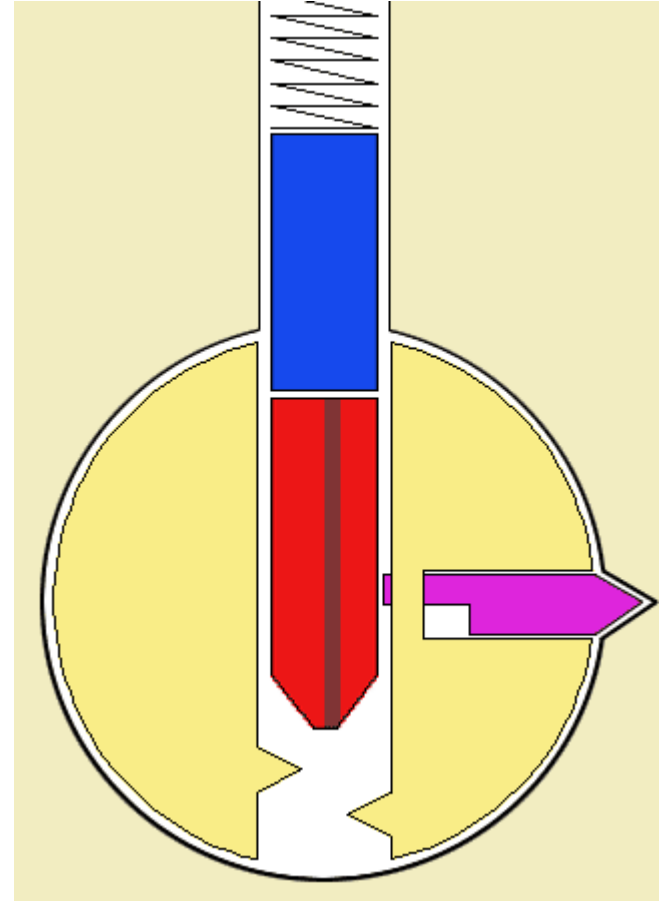
Side Bars

Sliders



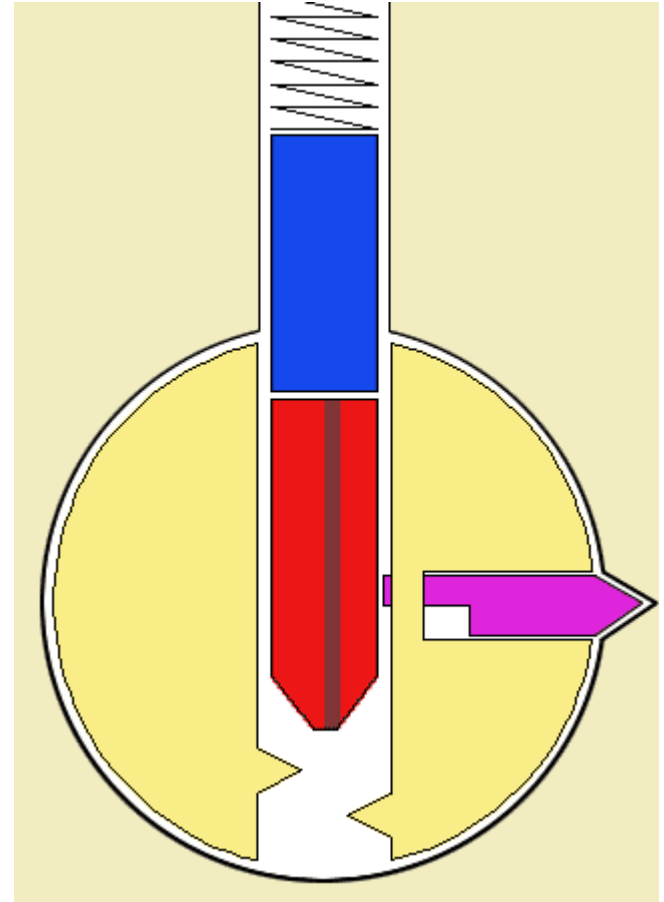
Side Bars

Rotating Pir



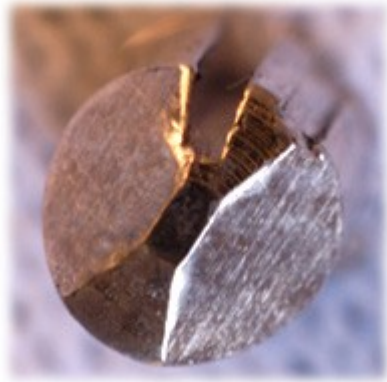
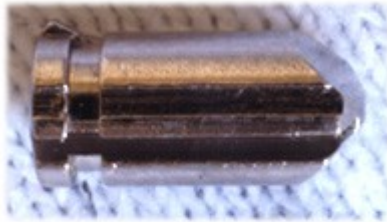
Side Bars

Rotating Pir



Rotating Pins

Medeco Locks



Medeco plug exposed, key pins rotating to align sidebar cuts



Top View



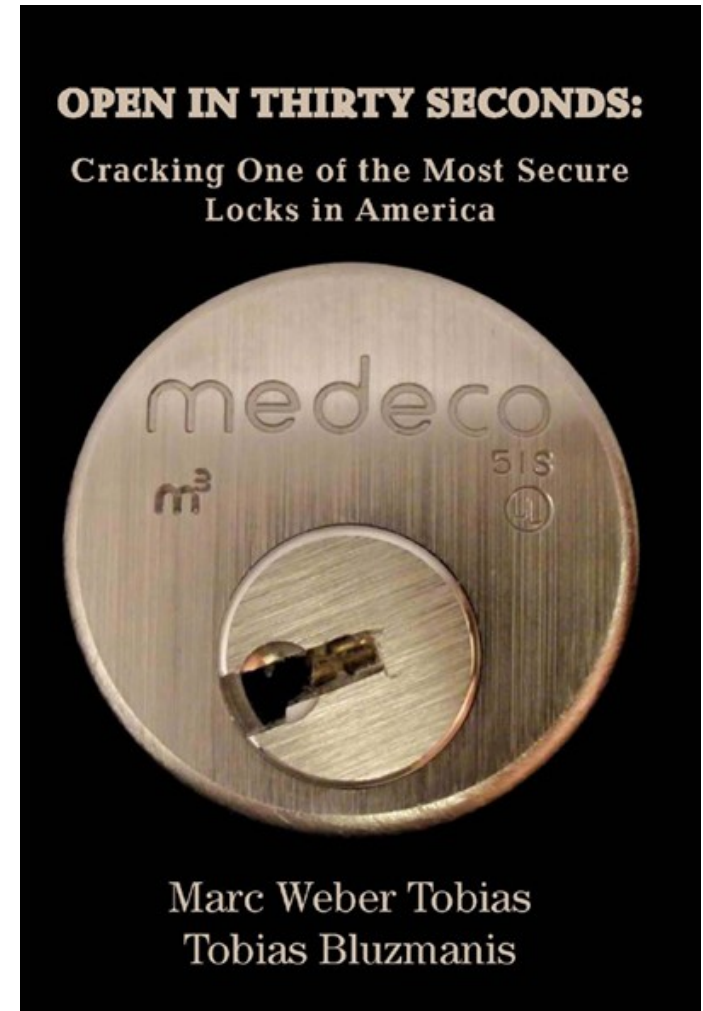
Side View

Rotating Pins

Medeco Locks

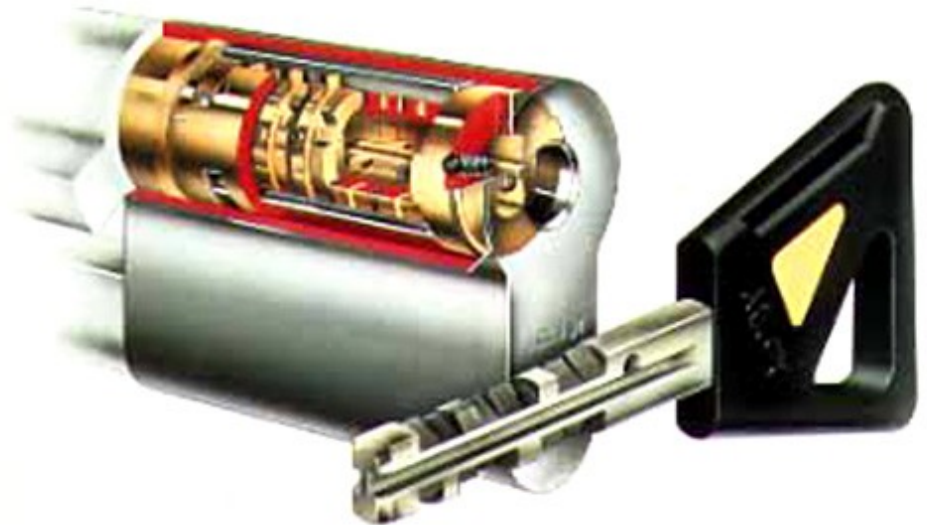
Totally shot now

- Can be picked
 - Can be bumped
 - Numerous weaknesses
- **“Open in 30 Seconds”**
 - Marc Tobias
 - Tobias Bluzmanis



Rotating Disks

- **Tremendous Security**
 - Mimics a safe lock
- **Very Difficult To Pick**
 - Takes much time and great skill
 - Specialized tools required



Rotating Disks

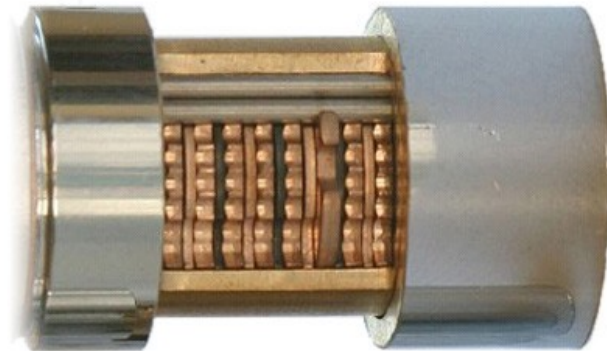
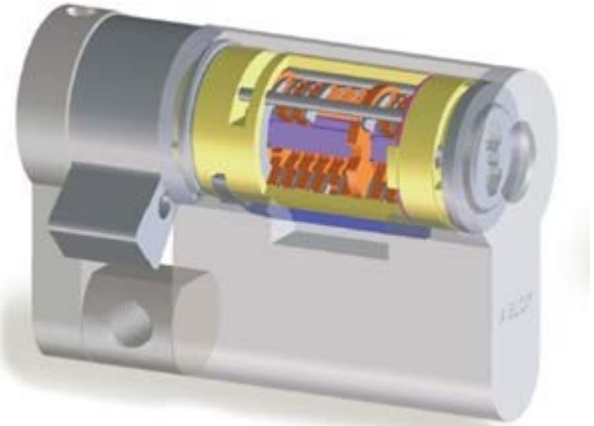
- **Tremendous Security**
 - Mimics a safe lock
- **Very Difficult To Pick**
 - Takes much time and great skill
 - Specialized tools required
- **Two-in-One Tool**
 - Manipulates disks individually
 - Decodes cut positions



Barry Wels picking a rotating disk lock with Mike Glasser

Specialized Rotating Disks

- **Abloy Protec**
 - Not just rotating disks
 - Disk blocking mechanism
 - False cuts everywhere
- **“Unpickable?”**
 - Closest I ever come to using that word
 - Two-in-one tools cannot be used



Magnetic Locks

- **Miwa**

- Japanese company
- Array of magnetic pins
- Simple North / South

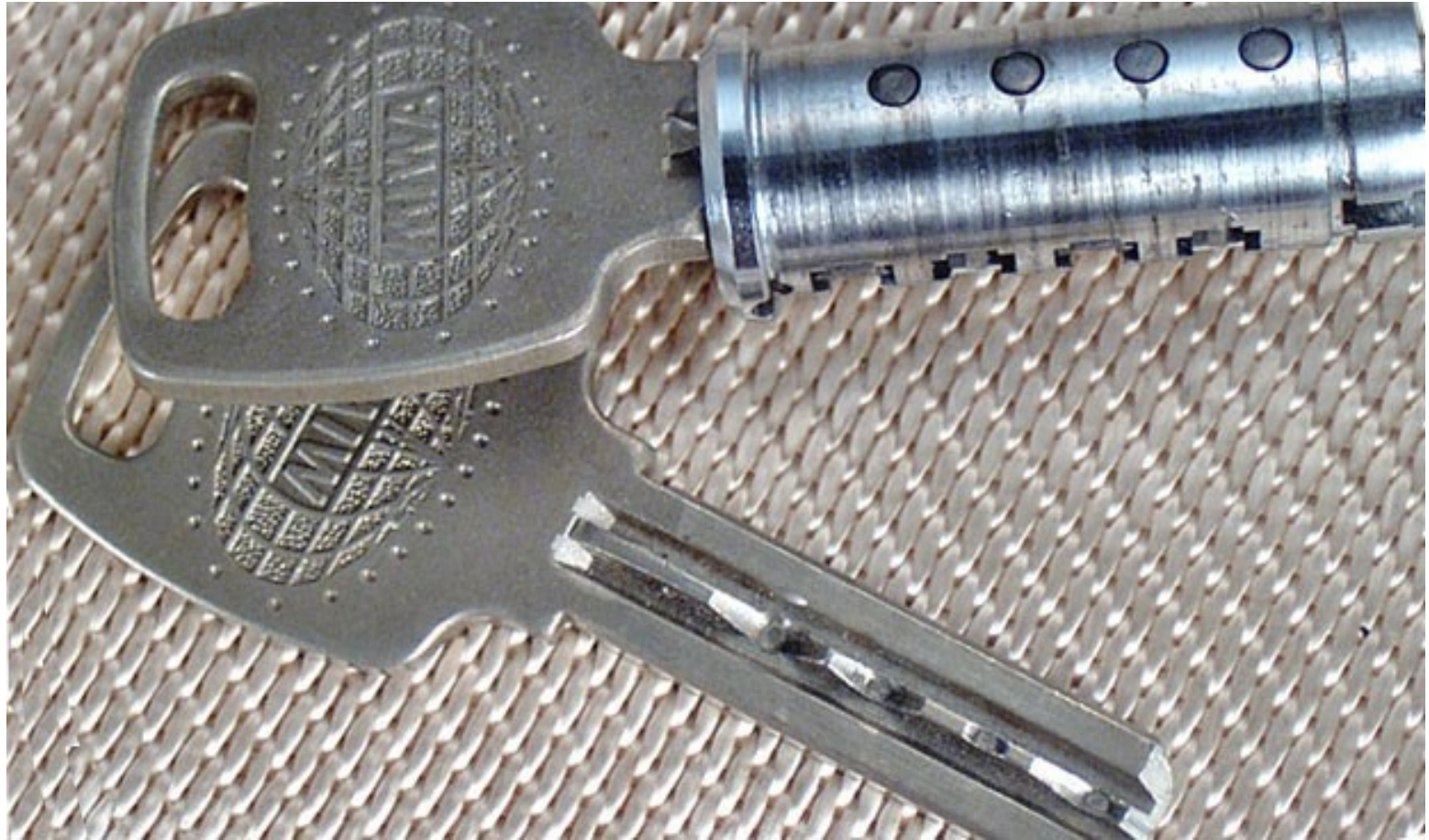


- **Evva MCS**

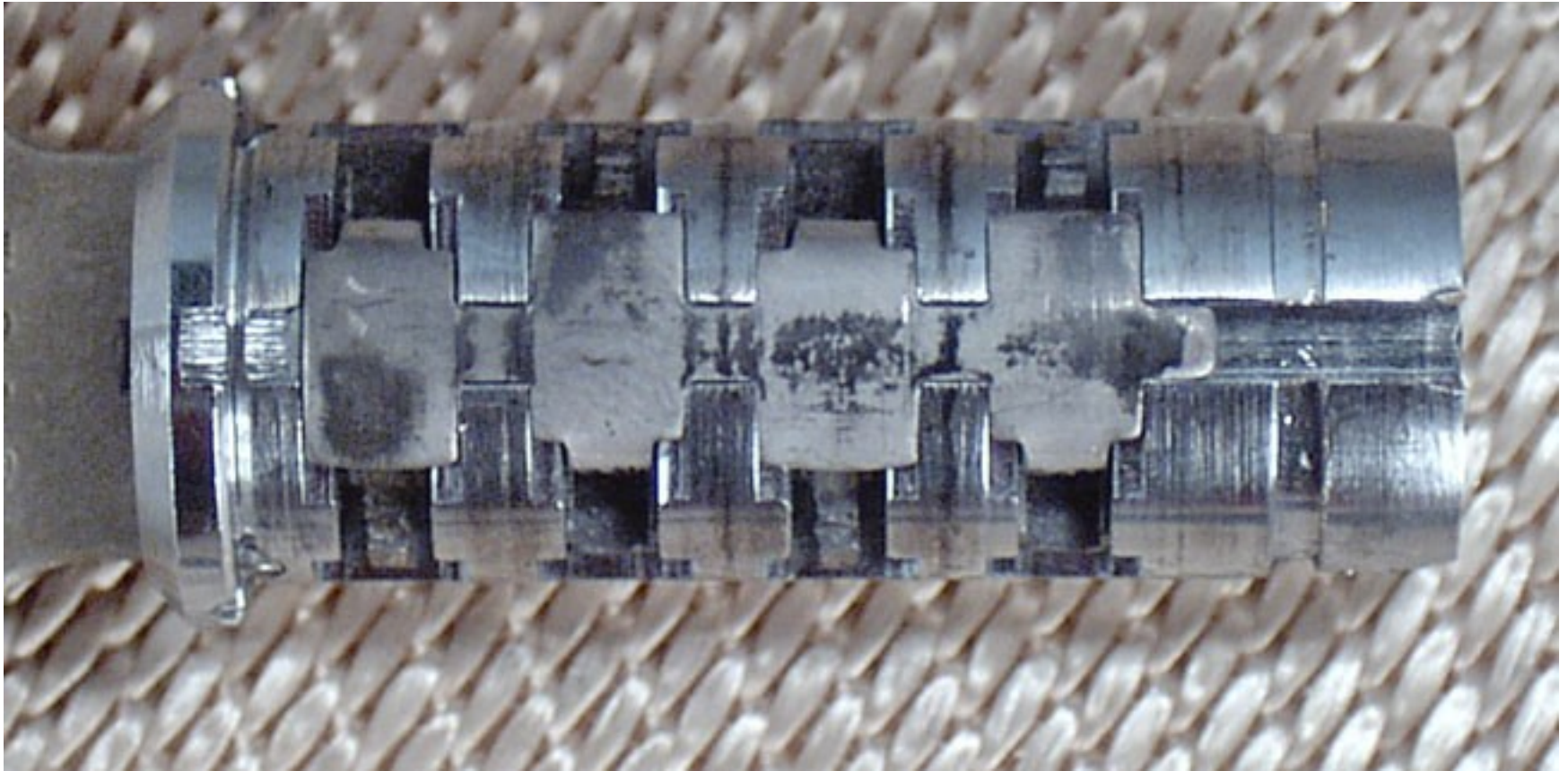
- Austrian company
- Axial-rotated magnets
- Interaction with sidebar



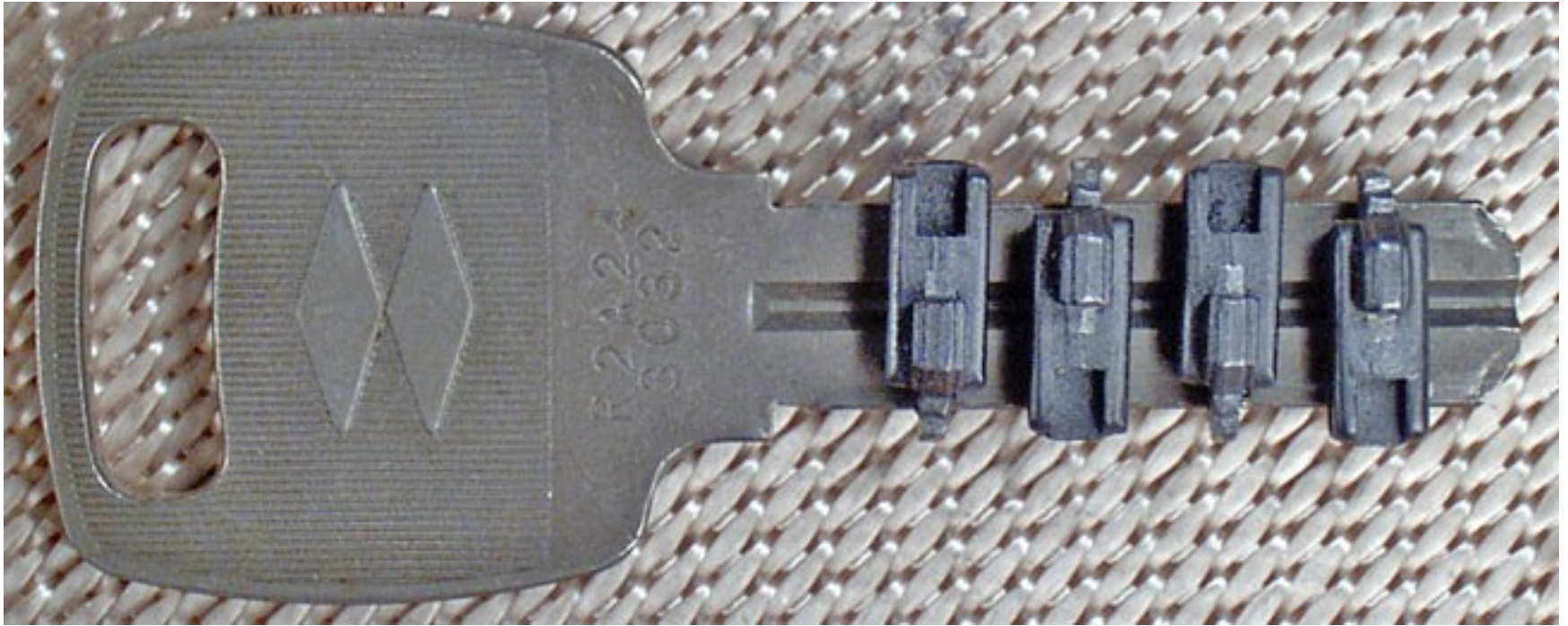
Miwa Magnetic Locks



Miwa Magnetic Locks

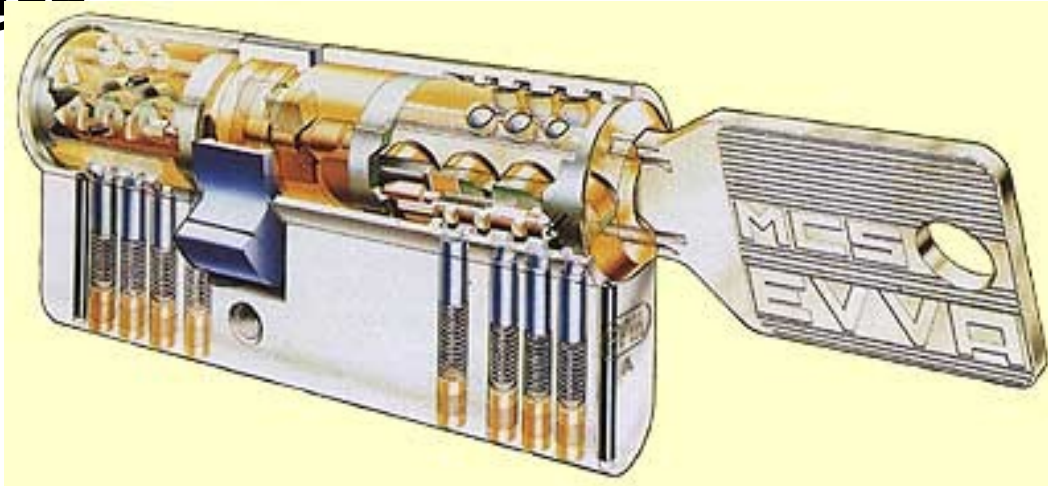


Miwa Magnetic Locks



Evva Magnetic Code System

- Possibly most duplication-resistant lock out there



Mul-T-Lock



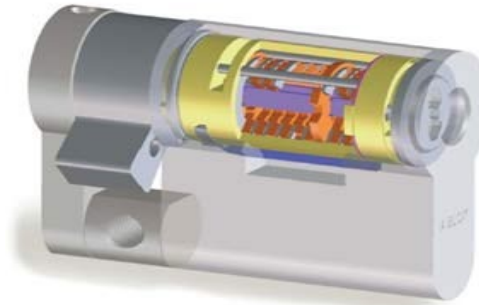
Mul-T-Lock



Mul-T-Lock



No Known Attack or Bypass



 **ABLOY**

**Prote
c**



EVVA

MCS



 **MTS+**
MUL-T-LOCK

Things You Should Know about Lockpicking...

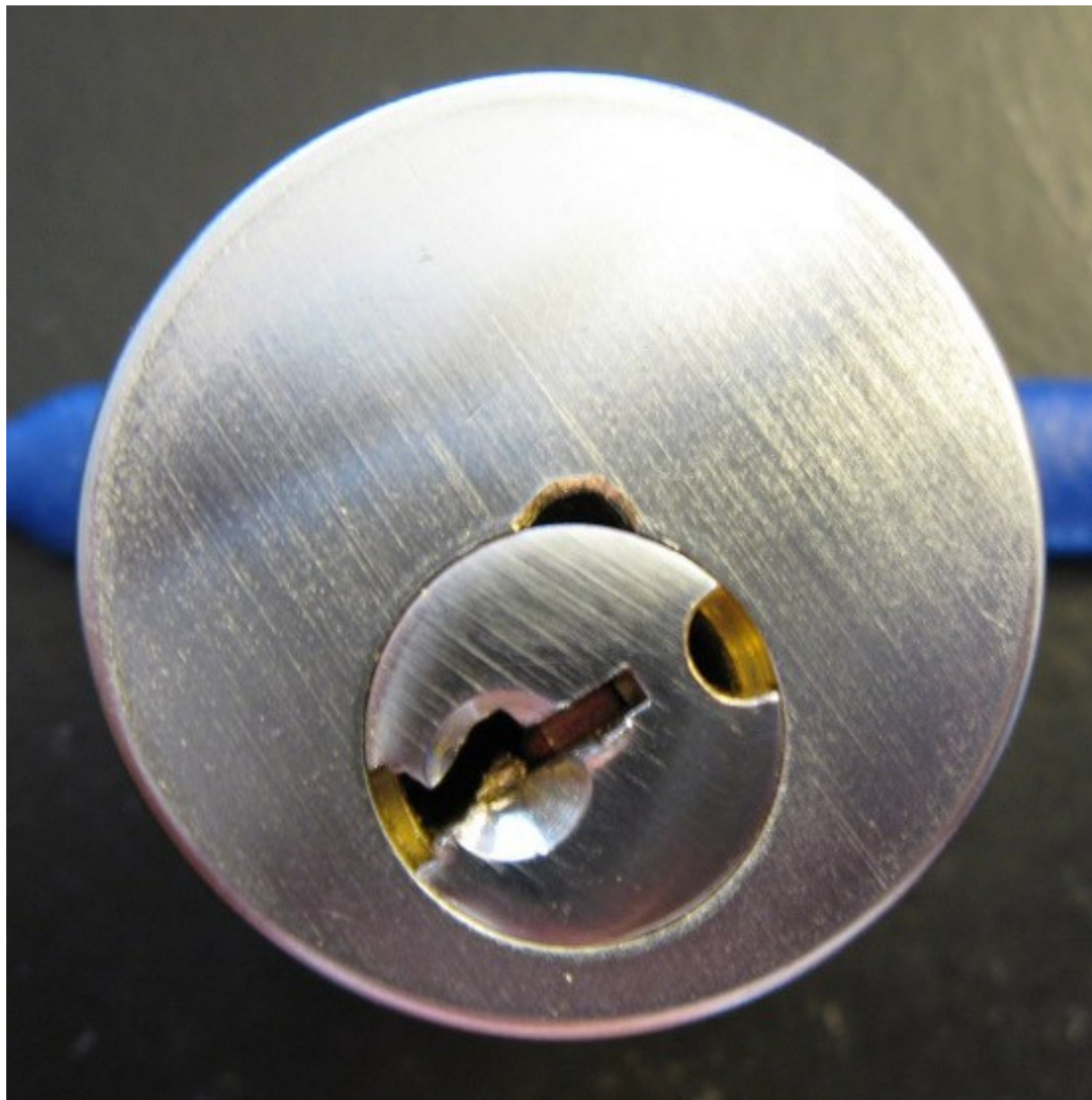
1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings















Most Attacks are Brute Force



Social Engineering



Social Engineering

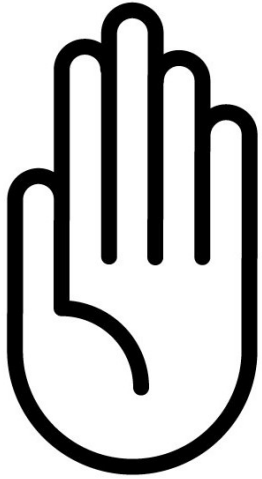


Social Engineering



Social Engineering

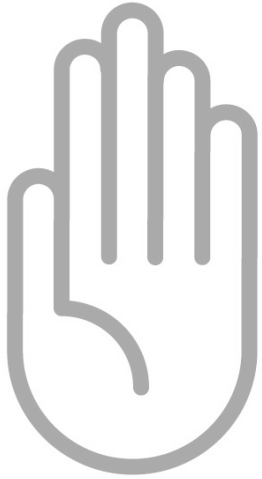
Preparedness



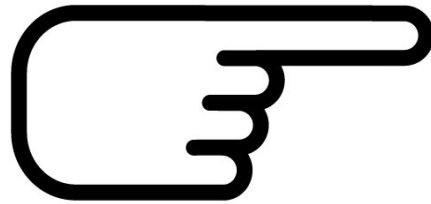
Stop

Social Engineering

Preparedness



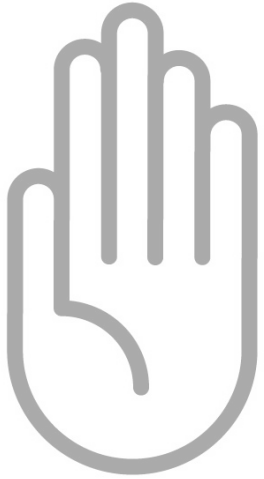
Stop



Challenge

Social Engineering

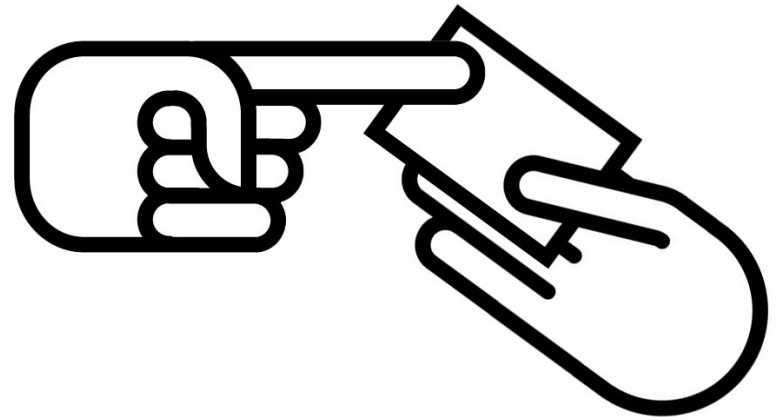
Preparedness



Stop



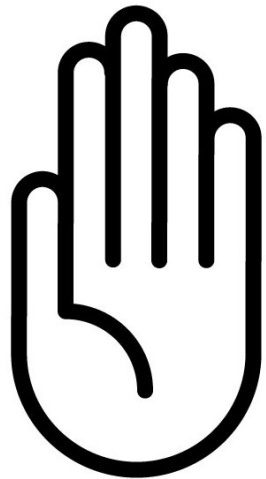
**Challe
nge**



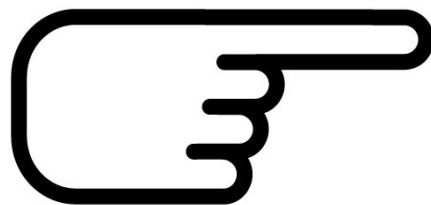
**Authenti
cate**

Social Engineering

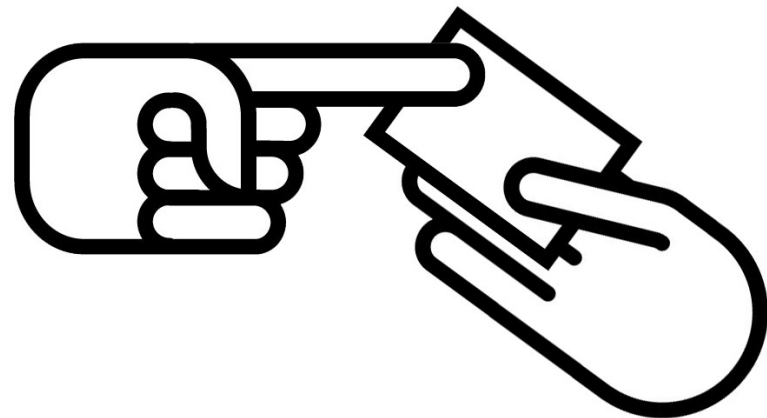
Preparedness



Stop



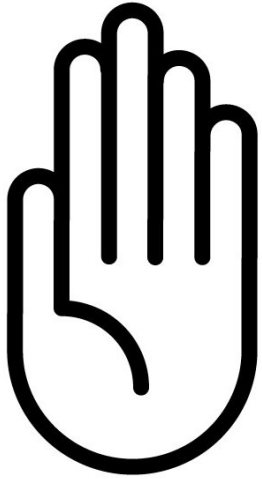
**Challe
nge**



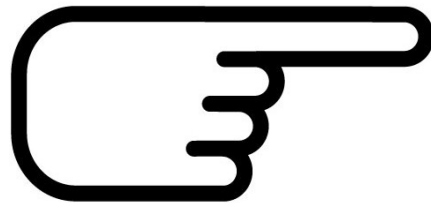
**Authenti
cate**

Social Engineering

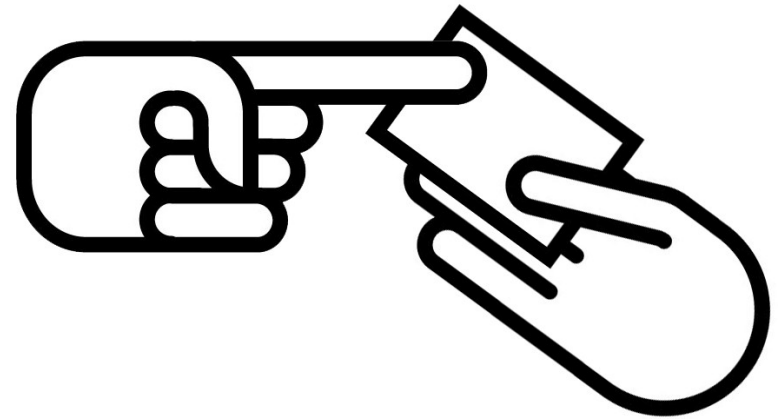
Preparedness



Stop



**Challe
nge**



**Authenti
cate**

**... then you follow this
with “Reward”**

Social Engineering



Social Engineering



Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings

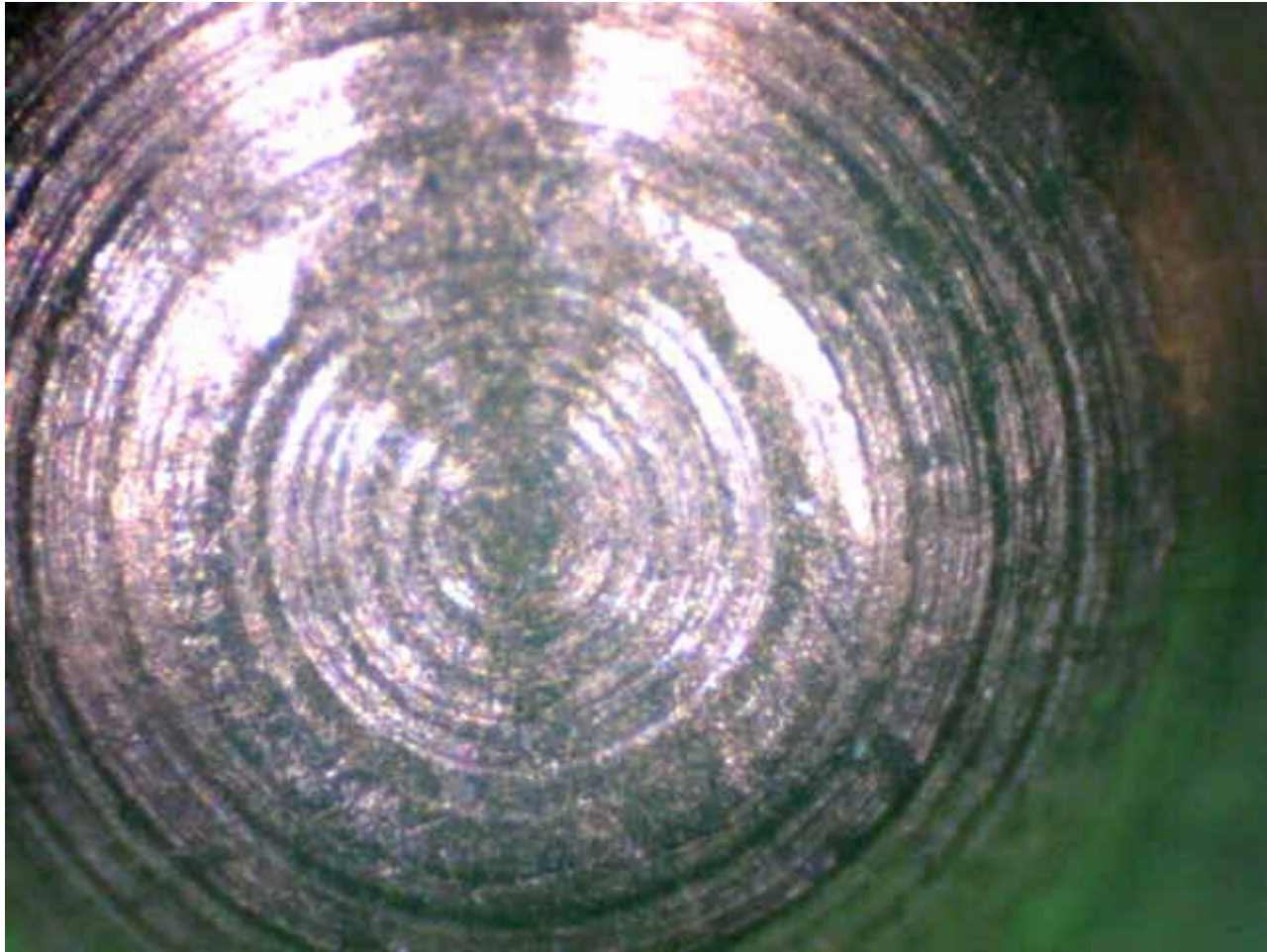
Forensic Evidence



Forensic Evidence



Forensic Evidence



Forensic Evidence - 250 uses



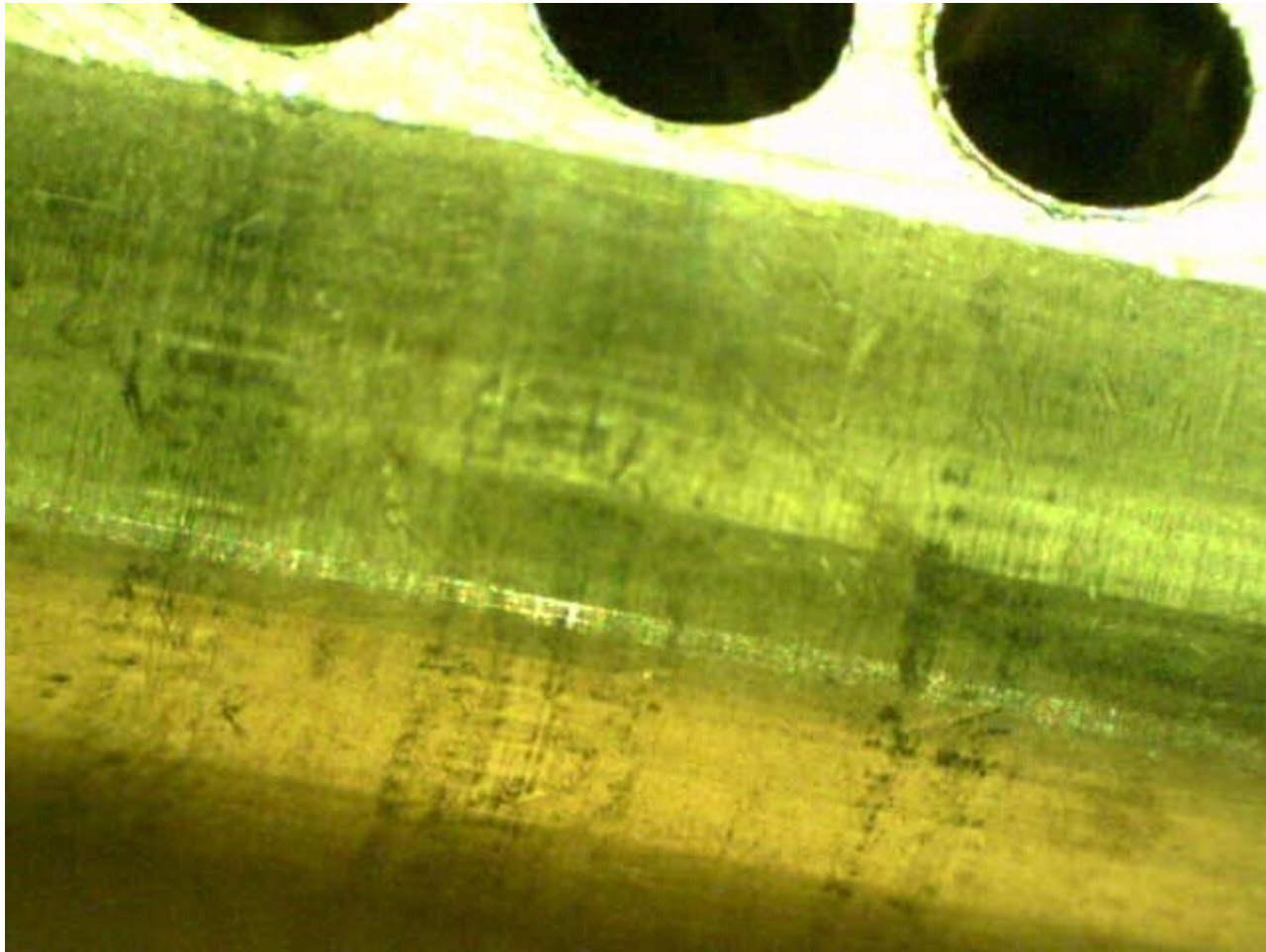
Forensic Evidence - 1,500 uses



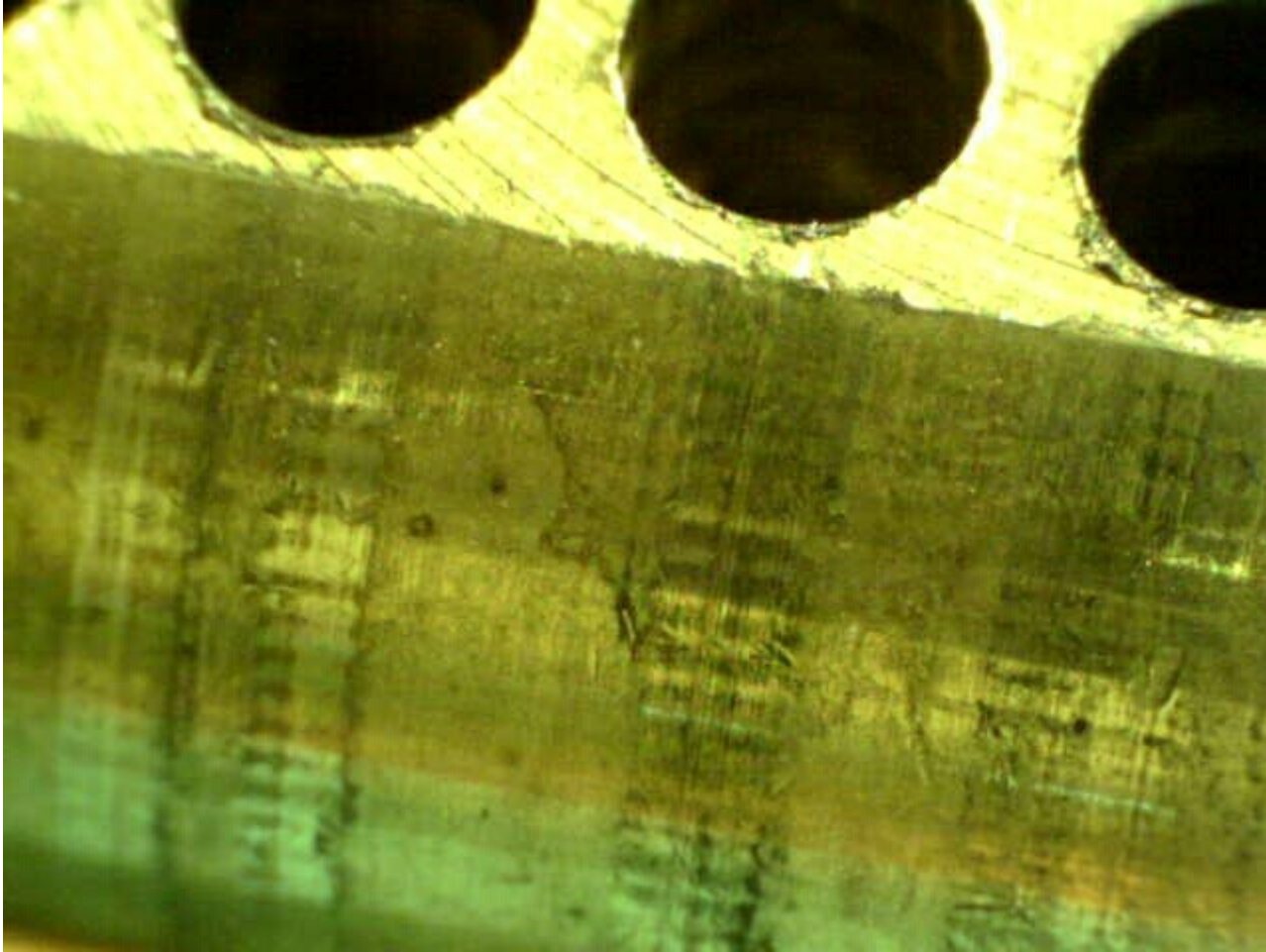
Forensic Evidence - 5,000 uses



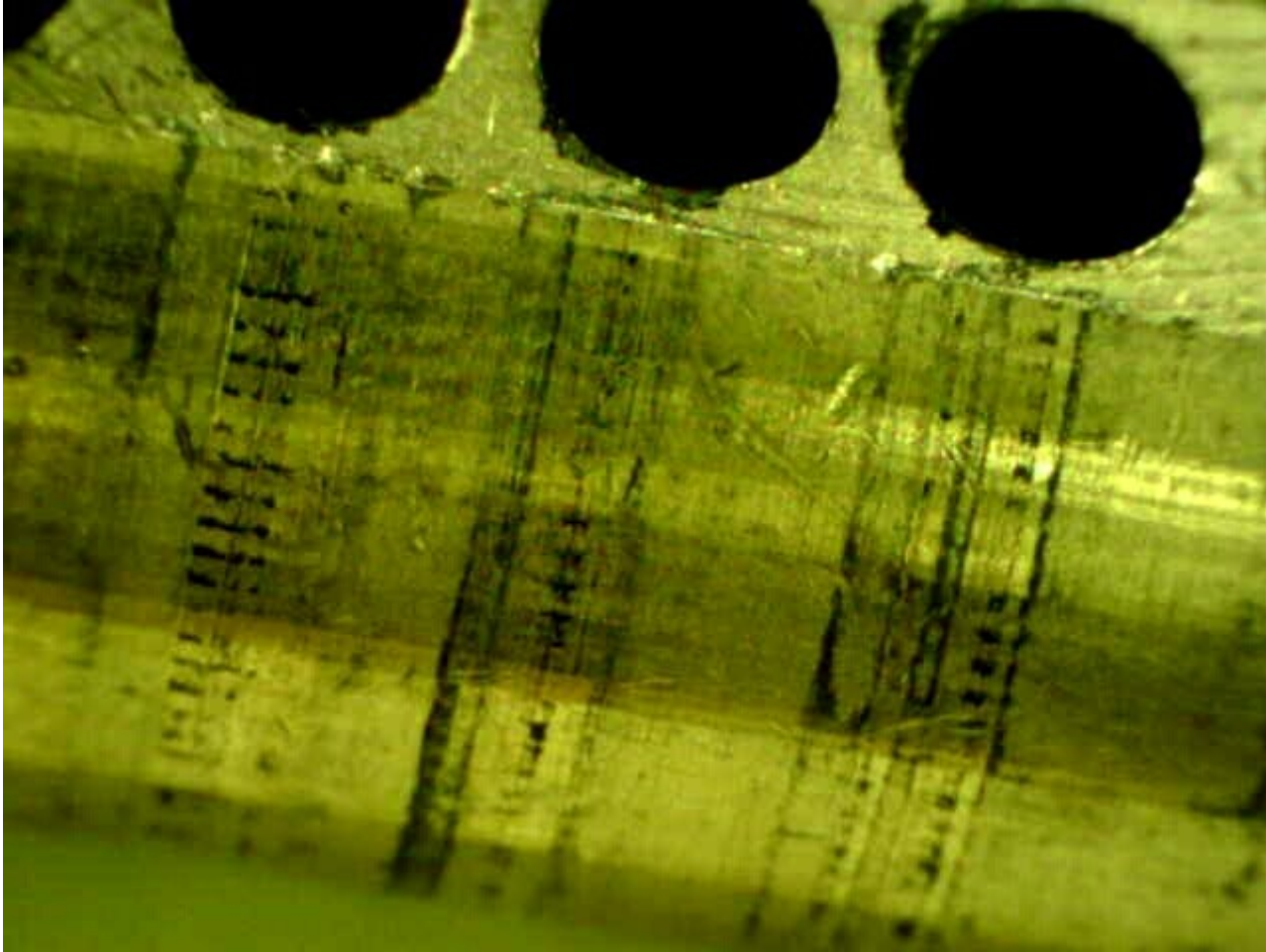
Forensic Evidence - 250 uses



Forensic Evidence - 1,500 uses



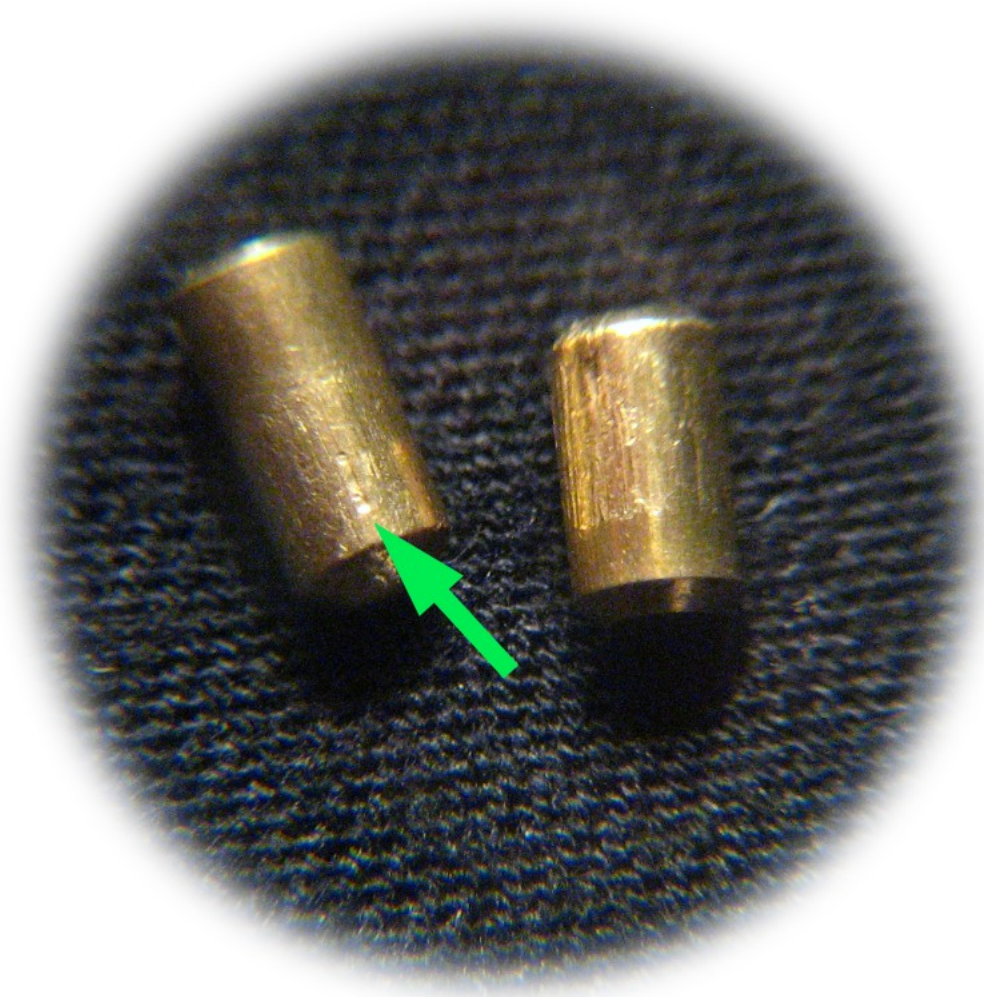
Forensic Evidence - 5,000 uses



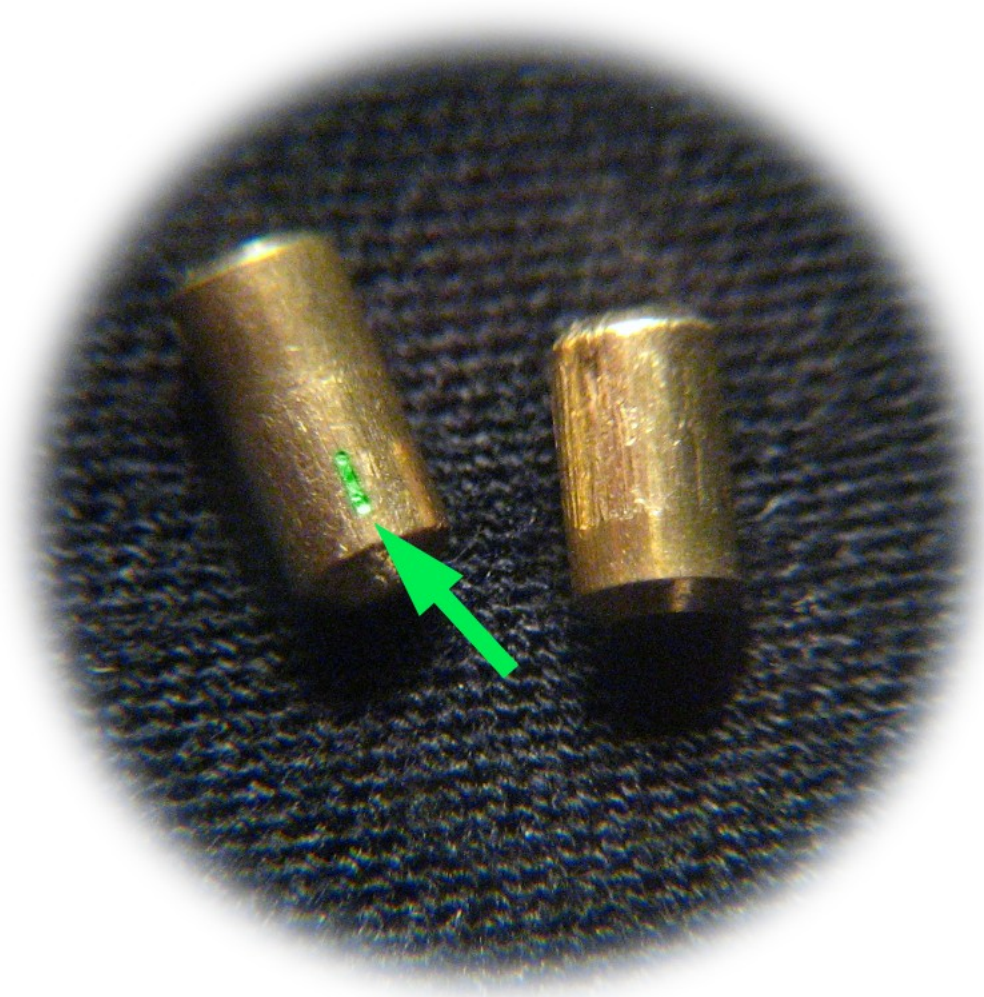
Forensic Evidence



Forensic Evidence



Forensic Evidence



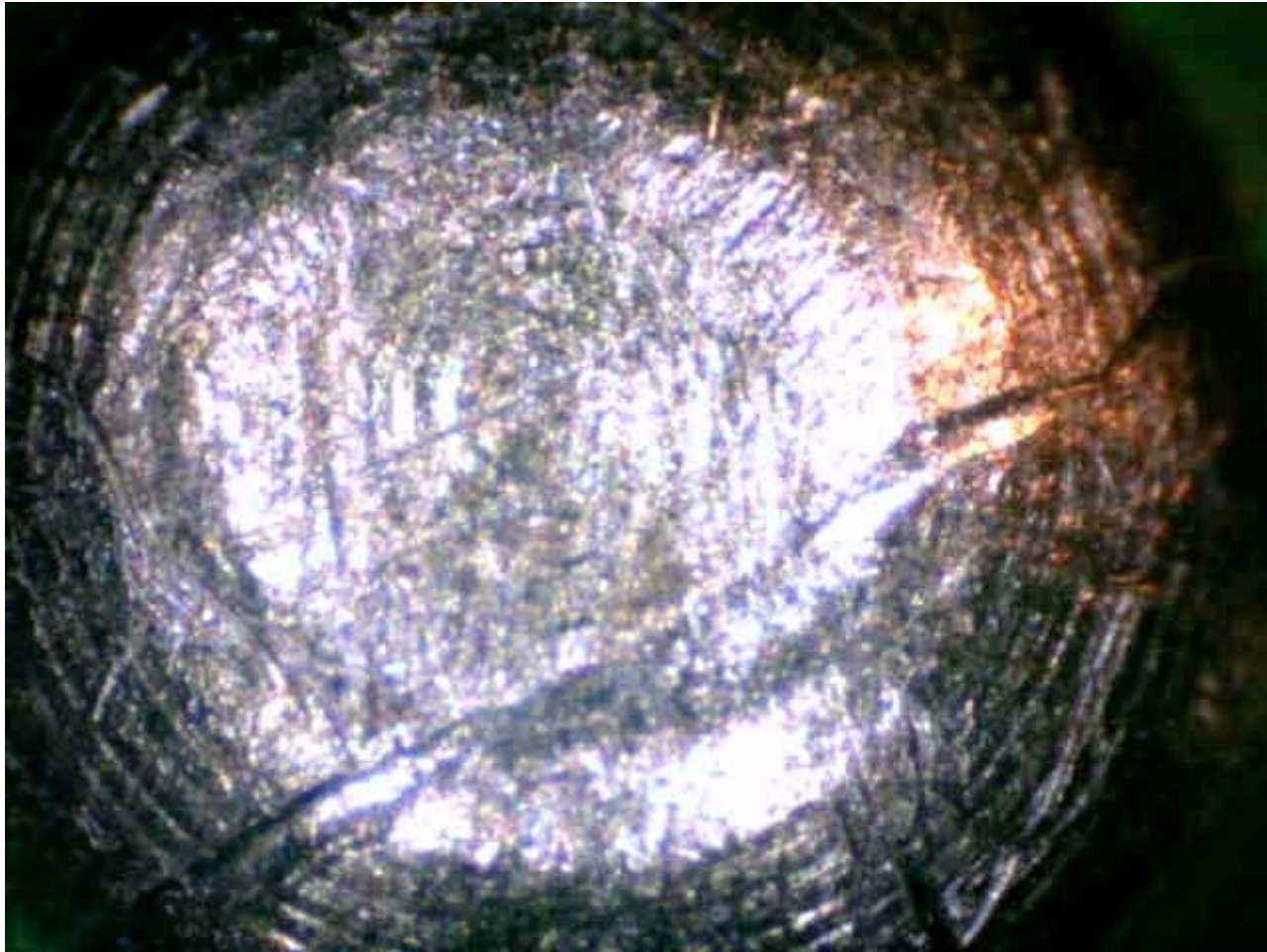
Forensic Evidence



Forensic Evidence - picking



Forensic Evidence - raking



Forensic Evidence - both



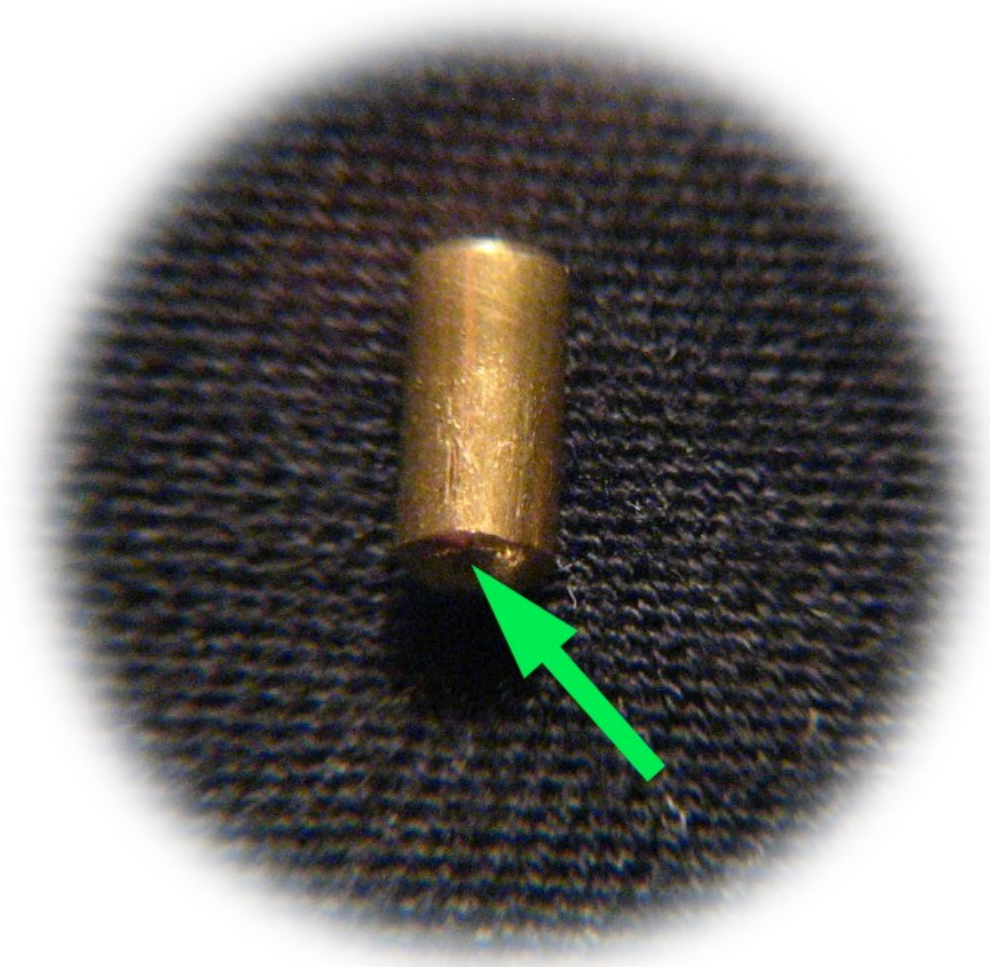
Forensic Evidence - ugh



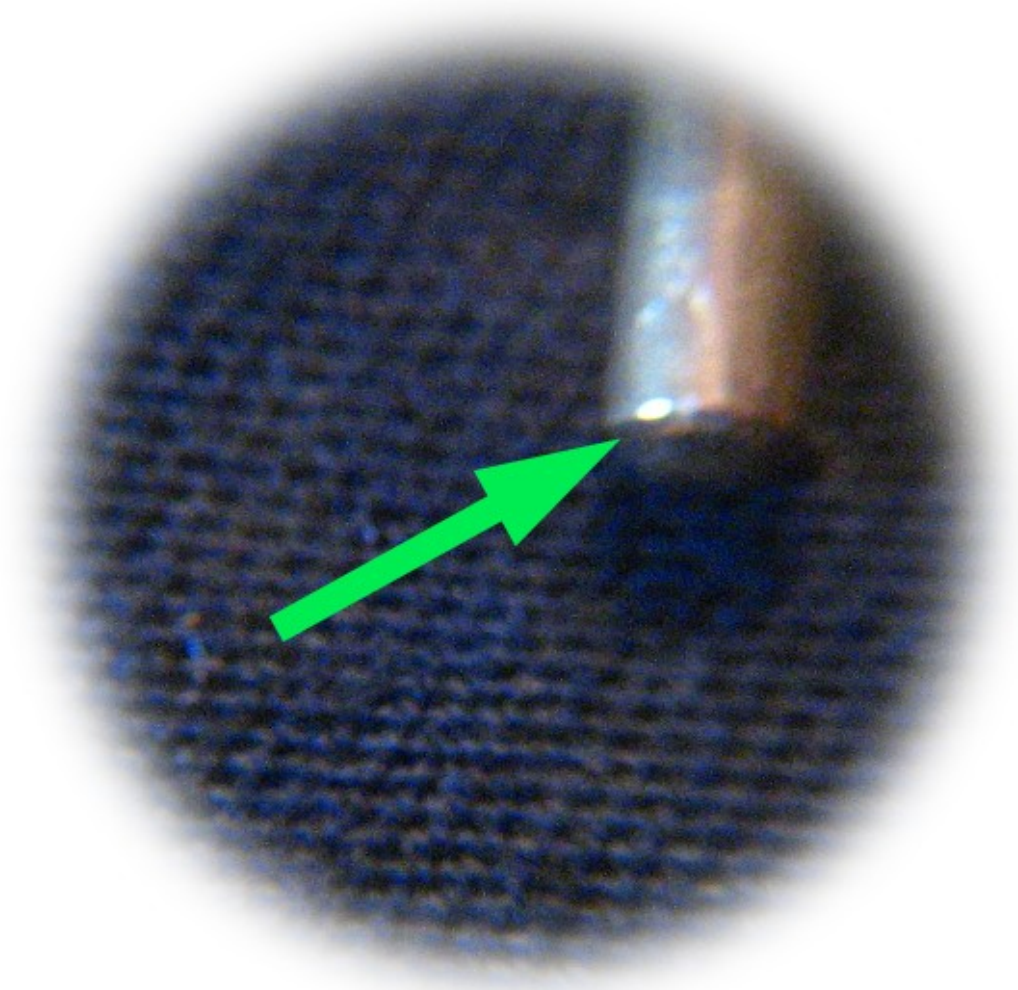
Forensic Evidence - wow



Forensic Evidence



Forensic Evidence



Forensic Evidence - bumping



Forensic Evidence - bumping



Security is only as effective



Thank you very much.



Special thanks to T000L, Babak, and Daisy

<http://deviating.net>

T000L this presentation is CopyLeft by Deviant Ollam, you are free to reuse any or all of the materials herein as it is attributed in freedom for other so the same is maintained.
<http://enterthecore.net> <http://toool.us>